PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, 12/56 | A3

(11) International Publication Number: WO 97/00471

(43) International Publication Date: 3 January 1997 (03.01.97)

(21) International Application Number: PCT/IL96/00017

(22) International Filing Date: 16 June 1996 (16.06.96)

(30) Priority Data:
114182 15 June 1995 (15.06.95) IL

(60) Parent Application or Grant
(63) Related by Continuation
US 08/168,041 (CIP)
Filed on 15 December 1993 (15.12.93)

(71) Applicant *(for all designated States except US)*: CHECK POINT SOFTWARE TECHNOLOGIES LTD. [IL/IL]; Hateomim Building 2, 35 Jabotinsky Street, 52511 Ramat Gan (IL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SHWED, Gil [IL/IL]; 21 Harechesh Street, 69699 Tel Aviv (IL). KRAMER, Shlomo [IL/IL]; 36 Harav Kuk Street, 63302 Tel Aviv (IL). ZUK, Nir [IL/IL]; 2 Zvi Street, 52504 Ramat Gan (IL). DOGON, Gil [IL/IL]; 78 Hakidma Street, 46743 Hertzlia (IL). BEN-REUVEN, Ehud [IL/IL]; 11 Arba Aratzot Street, 62486 Tel Aviv (IL).

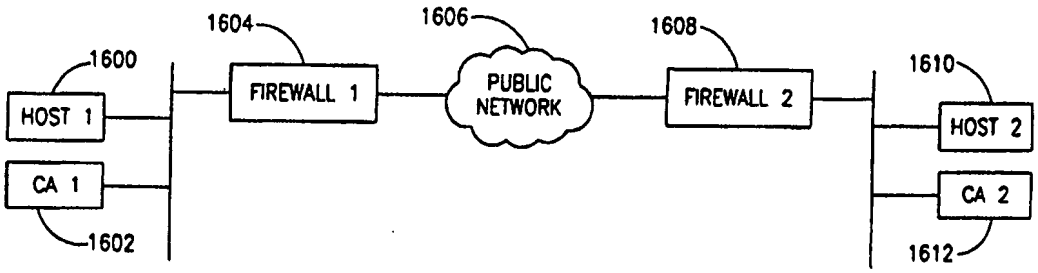
(74) Agent: A. TALLY EITAN-ZEEV PEARL & CO.; Lumir House, 22 Maskit Street, 46733 Herzlia (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
6 March 1997 (06.03.97)

(54) Title: A SYSTEM FOR SECURING THE FLOW OF AND SELECTIVELY MODIFYING PACKETS IN A COMPUTER NETWORK



(57) Abstract

A novel system for controlling the inbound and outbound data packet flow in a computer network by which private networks can be secured from outside attacks. A user generates a rule base (400) which is converted into a set of filter language instructions where each rule includes a source, destination, service, whether to accept or reject the packet and whether to log the event. The filter language instructions are executed on inspection engines (204) on computers acting as firewalls (124) positioned in the network such that all traffic is forced to pass through the firewall. Packets are filtered in accordance with the rule base. The inspection engine acts as a virtual packet filter machine (600) determining whether to accept or reject a packet. If a packet is rejected, it is dropped, and if accepted may be modified. Modifications, performed in accordance with the rule base, may include encryption, decryption, signature generation or verification, or address translation.

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－504168

(43)公表日　平成10年(1998)４月14日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５

審査請求　未請求　予備審査請求　有　（全 77 頁）

(21)出願番号　特願平9－502876
(86)(22)出願日　平成８年(1996)６月16日
(85)翻訳文提出日　平成９年(1997)２月17日
(86)国際出願番号　ＰＣＴ／ＩＬ９６／００００１７
(87)国際公開番号　ＷＯ９７／００４７１
(87)国際公開日　平成９年(1997)１月３日
(31)優先権主張番号　１１４１８２
(32)優先日　1995年６月15日
(33)優先権主張国　イスラエル（ＩＬ）

(71)出願人　チェックポイント・ソフトウエア・テクノロジーズ・リミテッド
イスラエル国ラマットガン52520・ヤボチンスキー　ストリートヤハロンタワー　３エイ
(72)発明者　シュウェド、ギル
イスラエル国テルアビブ69699・ハレチェシュストリート　21
(72)発明者　クレイマー、シュロモ
イスラエル国テルアビブ63302・ハラブクストリート　36
(74)代理人　弁理士　大島　陽一　（外１名）

最終頁に続く

(54)【発明の名称】　コンピュータネットワークにおける通信のセキュリティのためのデータパケットを検査し選択的変更を施す方法及びシステム及びそのシステムの操作方法

(57)【要約】
本発明は、コンピュータネットワークにおける到着及び発信データパケットフローを制御するための新規なシステムを開示するものである。コンピュータネットワークにおけるパケットフローを制御することによって、私設ネットワークから外界へのパケットフローを制御するとともに、私設ネットワークを外部からの不法な攻撃から保護し得る。ユーザはルールベースを生成し、このルールベースは一組のフィルタリング処理言語命令セットに変換される。このルールベースの各ルールは、ソース、デスティネーション、サービス、パケットを通過させるか拒絶するか、及びイベントを記録するか否かを定めるデータを含んでいる。このフィルタリング処理言語命令セットは、コンピュータ上に設置された検査エンジンにインストールされ、その上で実行されて、ファイヤウォールとして機能する。このファイヤウォールは、ネットワーク内を行き来する機密保護されるべき全てのトラヒックがこのファイヤウォールを通過せざるを得ないように、コンピュータネットワーク内に設置される。従って、パケットは、ネットワークに出入りするときにルー

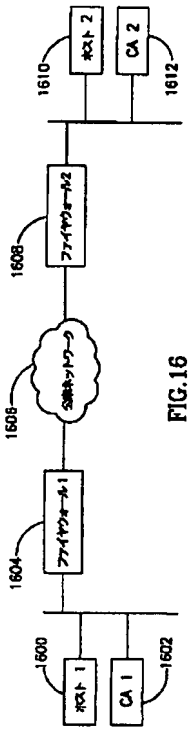


FIG.16

【特許請求の範囲】

1．コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法であって、

前記セキュリティルールによって検査された前記コンピュータネットワークの各アスペクトの定義を生成する過程と、

前記アスペクトの定義によって、前記アスペクトの少なくとも１つを制御する前記セキュリティルールを生成する過程と、

前記セキュリティルールを、前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すパケットフィルタリングモジュールの動作を制御するためのパケットフィルタリング処理言語命令セットに変換するセキュリティルール変換過程と、

前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すために、仮想パケットフィルタリングマシンを実現する前記パケットフィルタリングモジュールと、前記コンピュータネットワークを接続する過程と、

前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするコンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法。

2．前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項１に記載の方法。

3．前記アスペクトが、ネットワークサービスを含むことを特徴とする

請求項１に記載の方法。

4．前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項２に記載の方法。

5．前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレ

スを含むことを特徴とする請求項４に記載の方法。
６．前記セキュリティルール変換過程の前記フィルタリング処理言語命令セットが、スクリプトの形態であり、前記スクリプトを、前記パケットフィルタリング処理言語命令実行過程において実行される前記命令セットにコンパイルするコンパイラを含んでいることを特徴とする請求項１に記載の方法。
７．前記コンピュータネットワークの各アスペクトの定義を生成する過程、及び前記セキュリティルールを生成する過程の双方において、グラフィカルな定義がなされることを特徴とする請求項１に記載の方法。
８．前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項１に記載の方法。
９．コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、
前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも１つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、該過程と、
前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有する

ことを特徴とするセキュリティシステムを操作する方法。
１０．前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項９に記載の方法。
１１．前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項９に記載の方法。
１２．前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項１０に記載の方法。
１３．前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレスを含むことを特徴とする請求項１２に記載の方法。
１４．前記仮想パケットフィルタリングマシンが、データ抽出操作を実行することを特徴とする請求項９に記載の方法。
１５．前記仮想パケットフィルタリングマシンが、論理演算を実行することを特徴とする請求項１４に記載の方法。
１６．前記仮想パケットフィルタリングマシンが、比較処理を実行することを特徴とする請求項１５に記載の方法。
１７．前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項９に記載の方法。
１８．コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、
前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも１つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更

を施す仮想パケットフィルタリングマシンをエミュレートする、該過程と、

前記パケットフィルタリングモジュールが、パケットフィルタリング処理を実行するための前記パケットフィルタリング処理言語命令を読み出し、実行する過程と、

前記パケットフィルタリング処理言語命令を読み出し、実行する過程において得られた結果を記憶装置に格納する過程と、

前記パケットフィルタリングモジュールが、格納された前記結果を用いて、前記パケットフィルタリング処理言語命令に基づいた前記仮想パケットフィルタリングマシンの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記デー

タパケットを選択的変更を施す過程とを有することを特徴とするセキュリティシステムを操作する方法。

１９．前記アスペクトが、ネットワークオブジェクトを含むことを特徴とする請求項１８に記載の方法。

２０．前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項１８に記載の方法。

２１．前記アスペクトが、ネットワークサービスを含むことを特徴とする請求項１９に記載の方法。

２２．前記アスペクトたる前記オブジェクトの定義が、前記オブジェクトのアドレスを含むことを特徴とする請求項２１に記載の方法。

２３．前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項１８に記載の方法。

２４．コンピュータネットワークを行き来する到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって制御される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命

令に変換される、該セキュリティシステムにおいて、

前記セキュリティルールに従って動作し、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールと、

前記パケットフィルタリング処理言語命令を読み出し実行する、前記

パケットフィルタリングモジュールと一体化された処理手段であって、前記パケットフィルタリングモジュールの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す、該処理手段とを有することを特徴とするセキュリティシステム。

２５．前記選択的変更が、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択されることを特徴とする請求項２４に記載のセキュリティシステム。

２６．図面に記載された実施例と実質的に同一であることを特徴とする請求項１乃至２３の何れか１つに記載の方法。

【発明の詳細な説明】

コンピュータネットワークにおける通信のセキュリティのためのデータパケットを検査し選択的変更を施す方法及びシステム及びそのシステムの操作方法

発明の背景

本出願は、一般に、コンピュータネットワークの機密保護、即ちセキュリティを制御する方法に関する。詳述すると、本出願は、外部及び内部のデスティネーション（終点）から、及びそこへ向かってネットワーク上を流れる情報を制御するコンピュータネットワークセキュリティのための、容易に変更可能、若しくは拡張可能な方法に関する。

接続性、即ちコネクティビティとセキュリティとは、多くの組織のコンピューティング環境における２つの両立困難な目的である。典型的な最近のコンピューティングシステムは、数多くのサービスに透過的にアクセスできるネットワーク通信網の周りに構築される。このようなサービスはグローバルに利用可能であり、これが最近のコンピューティングソリューションの唯一の最も重要な特徴であろう。接続性に対する要求は、組織内部及びその外部の双方から要求されているものである。

ネットワークサービスを無許可の使用から保護することは、全ての組織にとって非常に重要なことである。例えば、ユニックスワークステーションはひとたびインターネットに接続されると全世界に全てのサービスを提供し、そのサービスは次のテーブル上の別のステーションにも提供される。現在の技術を用いると、１つの組織は不正アクセスに対する防備のために、外界または他のサイトへの全ての接続が不可能になるほどその接続性を犠牲にしなければならない。

高度なセキュリティの必要性が高まるにつれ、ネットワークリソースへのアクセスを制御する手段が管理上の優先すべき事項となってきた。また、コストを節約し、生産性を維持するために、アクセスコントロールは、単純に校正でき、ユーザ及びアプリケーションに対して透過的なものでなければならない。セットアップコスト及びテイクダウン時間を最小限にすることも重要な要素である。

パケットフィルタリングは、通過するトラヒックを制御することによって接続性を確保しつつセキュリティを与え、１つのネットワーク内、及び接続されたネットワーク間の双方において、イリーガルな通信が試みられることを防止する方法である。

従来のパケットフィルタリングのインプリメンテーションでは、固定フォーマットに従ったリストテーブルによりアクセスを特定することができる。この方法の自由度は、所定の組織のセキュリティポリシーを表すものに限定されている。また、この方法は、適用対象、即ちオブジェクトが、特定のテーブルにおいて規定されたプロトコル及びサービスの組に限定されている。この方法では、元のテーブルにおいて特定されていない異なるプロトコル若しくはサービスの導入が不可能なのである。

パケットフィルタリングを実現する他の方法では、その組織の各セキュリティポリシーについて、コンピュータオペレーティングシステムのコードを手で調整する。この方法での限界は、将来のネットワークトポロジーの変化、新たなプロトコルの使用、サービスの強化、及び将来セキュリティが脅かされる可能性に対処できる自由度がないことである。この方法では、コンピュータプログラムを適切なものに変更するために専門家による大量の作業が必要であることがシステムの欠点であって、システムのセットアップ及び維持にコストがかさむ。

更に、企業、支社、及びビジネス上のパートナーとの間の長距離の通信のセキュリティの必要性は、近年のビジネスの現実においては不可欠なものにまで高まってきている。歴史的には、完全に私設の企業間の長距離の業務処理のためには、ネットワーク間のポイントツーポイント接続が用いられた。しかし、このようなシステムでは自由度を欠き、法外なコストがかさむことから、広く使用されるには到らなかった。インターネットのような公衆ネットワークは、長距離のインターネットワーキング用の自由度の高い低コストのソリューションを提供する。専用ラインを確立する代わりに、インターネットを媒介物として使用することにより企業間の通信が可能である。ローカルなインターネットプロバイダにひとたび接続すると、私設ネットワークはたちまち世界中のデスティ

ネーションに接続することが可能になる。

なんらかの公衆セグメントを使用する私設ネットワークは、仮想私設ネットワーク、またはバーチャルプライベートネットワーク（ＶＰＮ）と呼ばれる。ＶＰＮは専用私設ネットワークと較べて極めて低コストで自由度が高い。各施設ネットワークは、ローカルインターネットプロバイダに接続するだけでよい。新たな接続を加えることも、簡単でコストがかからない。しかし、ＶＰＮの主な欠点は、セグメントのなかにセキュリティを施されていないところも含まれるため機密保護の安全性を欠くことである。インターネットへの接続は、その企業を２つの危険にさらす。それは、（１）企業内ネットワークへの不当なインターネットアクセス（ブレークイン）、及び（２）インターネット内を通過していく企業通信の傍受及び干渉である。

インターネット上の通信に伴うセキュリティのリスクがあることによって、企業はＶＰＮの利点を完全に享受できない。インターネット上でビジネスを実行するために（即ち、送金、クレジット情報の獲得及び認証、製品の販売及び配布）には、信頼性が高く効果的なセキュリティを施すソリューションが必要なのである。

発明の要約

従って、米国特許出願第０８／１６８，０４１号の一部継続出願である本発明の目的は、コンピュータネットワーク内の情報フローを制御する、改善された、柔軟性を有し容易に変更が可能なセキュリティメソッドを提供することである。

本発明の別の目的は、ネットワーク上で内部及び外部のデスティネーションとの間を行き来する情報フローを、情報の暗号化、ソース及び／若しくはデスティネーションアドレスの変更の少なくとも一方の処理を含む形で制御することである。

本発明の更に別の目的は、システム内のノードを通過する暗号化された情報パケットを各パケット毎に検査することができるパケットフィルタによって情報フローを制御することである。

本発明の更に別の目的は、好ましくは非破壊接続有効性検査の後に、予め許可されたパケットのみを通過させることができるパケットフィルタによって情報フローを制御することである。

本発明の更に別の目的は、ノードにおける所定の、パケットを受容する（通過させる）か拒絶する（破棄する）かを定めるセキュリティ方針を実現する命令セットによって制御される、予め許可されたパケットのみを通過させる汎用パケットフィルタモジュールを提供することである。

本発明の更に別の目的は、システム管理者による変更が容易で、その変更に際してパケットフィルタ自体の特性の変更や大量のコードの書き込みが不要な、コンピュータネットワーク用セキュリティメソッドを提供することである。

本発明の更に別の目的は、改善された接続有効性チェック機構を提供することである。

本発明の更に別の目的は、何らかの暗号化手段、即ちデスティネーションアドレスの変更、受信基準としての外部入力の受け取り、及びネットワーク通信の拒絶または変更によりパケットを変更する能力を付与することである。

本発明の更に別の目的は、インターネットのような機密保護がなされない公衆ネットワーク上でのデータフローの機密保護のための暗号化スキームを提供し、仮想私設ネットワーク（ＶＰＮ）を構築できるようにすることである。

本発明の１つの側面によれば、暗号化によりネットワーク上のトランザクションの機密を保護し、異なるアドレス指定方法でさまざまなネットワーク間の相互接続をなし、また、通信のソースが許可を付与されており、ネットワーク上の通信の有効性が確認された場合にのみ、情報のパケットを通過させる方法を提供するとともに、それを達成するのに必要な情報が最小限ですみ、好ましくはフェールセーフ機能を備えたコンピュータシステムが提供される。

また、本発明の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法であって、前記セキュリティルールによって検査された前記コンピュータネットワークの各アスペクトの定義を生成する過程と、前記アスペクトの定義

によって、前記アスペクトの少なくとも１つを制御する前記セキュリティルールを生成する過程と、前記セキュリティルールを、前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すパケットフィルタリングモジュールの動作を制御するためのパケットフィルタリング処理言語命令セットに変換するセキュリティルール変換過程と、前記セキュリティルールに従って前記データパケットを検査し選択的変更を施すために、仮想パケットフィルタリングマシンを実現する前記パケットフィルタリングモジュールと、

前記コンピュータネットワークを接続する過程と、前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするコンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施す方法が提供される。

更に、本発明の１つのアスペクトとして、ネットワークオブジェクト、ネットワークサービス、若しくはその双方が含まれ得る。更に、オブジェクト定義はオブジェクトのアドレスを含み、また、セキュリティルール変更過程のフィルタリング処理言語命令はスクリプトの形態であって、そのスクリプトをコンパイルして、パケットフィルタリング処理言語命令実行過程において実行される命令に変換するコンパイラを更に含む。

更に、ネットワークのアスペクトを生成する過程、及びセキュリティルールを生成する過程の双方はグラフィック的に定義され、選択的変更処理は、暗号化、復号化、署名生成、及び署名確認からなる処理のグループから選択される。

また、本発明の別の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前

記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法におい

て、前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも１つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、該過程と、前記パケットフィルタモジュールが前記パケットフィルタリング処理言語命令を実行して前記仮想パケットフィルタリングマシンを操作し、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施すパケットフィルタリング処理言語命令実行過程とを有することを特徴とするセキュリティシステムを操作する方法が提供される。

また、本発明の更に別の好適実施例に基づき、コンピュータネットワークにおける到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって検査される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムを操作する方法において、前記セキュリティルールによって検査される前記コンピュータネットワークの少なくとも１つのエンティティにおいて、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールを設ける過程であって、前記パケットフィルタリングモジュールが、前記コンピュータネットワークに、または前記コンピュータネットワークから

出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタ

リングマシンをエミュレートする、該過程と、前記パケットフィルタリングモジュールが、パケットフィルタリング処理を実行するための前記パケットフィルタリング処理言語命令を読み出し、実行する過程と、前記パケットフィルタリング処理言語命令を読み出し、実行する過程において得られた結果を記憶装置に格納する過程と、

前記パケットフィルタリングモジュールが、格納された前記結果を用いて、前記パケットフィルタリング処理言語命令に基づいた前記仮想パケットフィルタリングマシンの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す過程とを有することを特徴とするセキュリティシステムを操作する方法が提供される。

更に、本発明の別の好適実施例に基づき、コンピュータネットワークを行き来する到着及び発信データパケットを、セキュリティルールに従って検査し選択的変更を施すセキュリティシステムであって、前記セキュリティルールによって制御される前記コンピュータネットワークの各アスペクトが予め定義されており、前記セキュリティルールが前記アスペクトによって前もって定義されており、かつパケットフィルタリング処理言語命令に変換される、該セキュリティシステムにおいて、前記セキュリティルールに従って動作し、前記コンピュータネットワークに、または前記コンピュータネットワークから出入りする前記データパケットを検査し選択的変更を施す仮想パケットフィルタリングマシンを実現する、前記コンピュータネットワークに接続されたパケットフィルタリングモジュールと、前記パケットフィルタリング処理言語命令を読み出し実行する、前記パケットフィルタリングモジュールと一体化された処理手段であって、前記パケットフィルタリングモジュールの操作を行い、前記コンピュータネットワークから、または前記コンピュータネットワークへの前記データパケットの出入りを受容若しくは拒絶し、そのようにして受容された前記データパケットを選択的変更を施す、該処理手段とを有することを特徴とするセキュリティシステムが提供される。

図面の簡単な説明

第１図は、ネットワークトポロジーの一例である。

第２図は、第１図のトポロジーのネットワークに適用された本発明のセキュリティシステムを示した図である。

第３図は、第２図のネットワーク管理部のコンピュータスクリーン上の表示を詳細に示した図である。

第４図は、グラフィカル情報をフィルタリング処理スクリプトに変換するサブシステムの流れ図である。

第５図は、本発明を利用したコンピュータネットワーク上での情報の流れを示す流れ図である。

第６図は、第５図に示すパケットフィルタの動作を示す流れ図である。

第７図は、第６図に示す仮想フィルタリングマシンの動作を示す流れ図である。

第８図は、第７図のデータ抽出方法を示す流れ図である。

第９図は、第７図の論理演算を示す流れ図である。

第１０図は、第７図の比較処理を示す流れ図である。

第１１図は、メモリへのリテラル値の入力方法を示す流れ図である。

第１２図は、条件付き分岐操作を示す流れ図である。

第１３図は、算術演算またはビット単位の演算を示す流れ図である。

第１４図は、探索操作を示す流れ図である。

第１５図は、記録操作を示す流れ図である。

第１６図は、本発明に基づいて構築されたファイヤウォールを用いている構成の一例を示す高レベルのブロック図である。

第１７図は、セッション鍵の交換中に、２つのファイヤウォール間で転送されるデータを示す高レベルのブロック図である。

第１８図は、セッションデータの交換中に、暗号化処理を用いて他のファイヤウォールへパケットを転送するファイヤウォールによって実行されるプロセスを示す、高レベルの論理流れ図である。

第１９図は、セッションデータの交換中に、他のファイヤフォールからの暗号化されたパケットを受け取るファイヤウォールによって実行されるプロセスを示す、高レベルの論理流れ図である。

第２０図は、ベーシック鍵の交換中に、２つのファイヤウォール間で転送されるデータを示す高レベルのブロック図である。

第２１図は、本発明に基づいて構築されたファイヤウォール、及びクライアントパーソナルコンピュータを用いている構成の一例を示す高レベルのブロック図である。

第２２図は、セッション鍵の交換中に、クライアントパーソナルコンピュータとファイヤウォールとの間で転送されるデータを示す高レベルのブロック図である。

第２３図は、ベーシック鍵の交換中に、クランアントパーソナルコンピュータとファイヤウォールとの間で転送されるデータを示す高レベルのブロック図である。

詳細な説明

到着及び発信データパケットフローの防護

第１図を参照すると、ネットワークトポロジーの一例が示されている。この例においては、メインサイト１００が、ワークステーション１０２に実現されたシステム管理機構を含んでいる。このワークステーション

はネットワークに接続されており、このネットワークには、ワークステーション１０４、ルータ１１０、及びゲートウェイ１０６が含まれている。ルータ１１０は、衛星１１２を介してリモートサイトのゲートウェイ１２２に接続されている。ゲートウェイ１０６はルータ１０８を介してインターネットに接続されている。リモートサイト１２０はネットワークに接続されたワークステーション１２４を含み、このワークステーション１２４はゲートウェイ１２２を介してインターネットに接続されている。ここに示す特定の構成は一例として選択されたものに過ぎず、本発明が機能を発揮し得るネットワークの型を限定しようとするものではない。ネットワークがとり得る構成の数は実質的に無限であり、このような構

成をセットアップするための技術は当業者には周知である。本発明は実現可能な任意の形態の上で動作し得るものである。

第２図は、本発明のシステムが組み込まれた第１図のネットワークを示した図である。第２図において、第１図にも示されている構成要素は同じ符号を付して示した。図に示すように、システム管理部１０２は、制御モジュール２１０、パケットフィルタジェネレータ２０８、ディスプレイ２０６、及び記憶媒体２１２を含む。パケットフィルタ２０４は、システム管理部、第１図のワークステーション１０４、及びゲートウェイ１０６上にインストールされている。ゲートウェイ１０６は、このようなフィルタを２つ有し、１つはネットワークへの接続部に、他方はルータ１０８への接続部に設けられている。ルータ１０８及び１１０はそれぞれ、セキュリティシステムによって生成されたプログラミングスクリプトテーブルを有しているが、これは本発明の一部分を構成するものではなく、詳細については説明しない。当業者には周知のように、これらのテーブルは、ルータをプログラムするのに従来より用いられてきたテーブルに対応するものである。

パケットフィルタ２０４は、リモートサイト１２０のゲートウェイ１２２上にもインストールされている。パケットフィルタの１つは、衛星１１２とゲートウェイ１２２との間のコネクション上にインストールされており、第２のパケットフィルタはインターネットとゲートウェイ１２２との間のコネクション上にインストールされており、第３のパケットフィルタはゲートウェイとネットワークとの間のコネクション上にインストールされている。

当業者には周知のように、情報はネットワーク上をパケットの形態で流れる。第２図におけるパケットフィルタの位置は、ワークステーション、ルータ、またはゲートウェイのようなネットワーク上の特定の対象機器、即ちオブジェクトからのデータフロー、若しくはその特定のオブジェクトへのデータフローを制御できるように選択される。従って、第１図のワークステーション１０４のそれぞれはパケットフィルタを有し、これらのワークステーションへの情報の流れ、若しくはこれらのワークステーションからの情報の流れは個別に制御される。しかし、リモートサイト１２０において、パケットフィルタはゲートウェイ１２２と

ネットワークとの間のコネクション上に設置されており、従ってワークステーション１２４へのデータフロー、若しくはそのワークステーションからのデータフローを個別に制御することはできない。このような個別化された制御が必要な場合は、同様にパケットフィルタを各ワークステーション１２４上に設置することができる。各パケットフィルタはネットワークのセットアップ時、若しくはセキュリティシステムのインストール時にインストールされるが、追加的なパケットフィルタを後日インストールすることも可能である。このパケットフィルタは、防護の必要なワークステーション若しくはゲートウェイ等のホストデバイス上にインストールされる。

各パケットフィルタはシステム管理部１０２におけるパケットフィルタジェネレータ２０８によって生成された命令セットに基づいて動作する。これらの命令セットによって、単にパケットの通過許可若しくは不許可についてのパラメータを含むテーブルに対してパケットの内容をチェックするのではなく、そのパケットについて複雑な操作を施すことが可能となる。従って、各パケットフィルタは、パケットフィルタ自体の構造を変化させることなく、複数のセキュリティルールを取り扱うとともに、極めて柔軟にセキュリティルールの変更を行うことができることになる。

システム管理者は、モニタ２０６上に表示されるグラフィカルユーザインタフェース（ＧＵＩ）を介してセキュリティルールを入力する。ＧＵＩについては第３図を参照しつつ後に詳しく説明する。この情報は、パケットフィルタジェネレータ２０８によって処理され、その結果得られたコードはネットワーク内の適切なパケットフィルタ若しくはフィルタに転送されて、所望の機能を発揮することになる。制御モジュール２１０により、システム管理者がネットワークの動作を追跡することが可能となり、また記憶媒体２１２によりネットワーク上の操作及びネットワークへの不法な侵入の試みの記録を保持しておくことが可能となる。これによって、システム管理者が、セキュリティルールがうまく機能を発揮しているか否かということや、ネットワークの動作に関する情報を完全に与えられ得

ることになる。従って、接続性を制限することなくネットワークのセキュリティを維持するための適切なネットワークの変更を、セイキュリティ管理者が施すことが可能となるのである。

第３図は、第２図コンピュータスクリーン２０６上の表示を詳細に示した図である。スクリーンは、４つのウィンドウに分けられており、左側には２つの小さいウィンドウが、右側には２つの大きなウィンドウが

配置される形となっている。ネットワークのオブジェクト（object）及びサービス（services）は、本発明のセキュリティメソッドにおいて規定されなければならないネットワークの２つのアスペクト（aspect）である。ウィンドウ３０４は、ワークステーション、ゲートウェイ、及びシステムに接続された他のコンピュータハードウェア等のネットワークオブジェクトを定めるために用いられる。いくつかのデバイスを、例えば、会社の財務部、研究開発部、及び経営者といったようにグループ化してまとめることも可能である。従って、パケットフィルタの適切な配置により、データフローの制御を、ネットワーク上の個別のコンピュータに対してのみならず、ネットワーク上のコンピュータのグループに対しても行うことが可能である。これにより、システムオペレータがネットワーク上の通信の管理に当たって自由度を大きくすることができる。例えば、会社の最高責任者（ＣＥＯ）や役員のような上層部の経営者は財務部のチーフと同様に財務部と直接通信を行うことができるが、他のグループからの通信はフィルタリングするようにすることができる。また、特定のコンピュータの組に対して、全てのグループからの電子メールを受け取ることができるが、それ以外の情報のリクエストを制限するようにすることもできる。これによってシステムオペレータが、そのネットワークの対外セキュリティと同様、内部的なセキュリティを施すことが可能となる。このオブジェクト定義は、ネットワーク上のオブジェクトのアドレスや、そのオブジェクトがネットワークの内部（internal）または外部（external）の何れに存在するか、パケットフィルタがそのオブジェクト上にインストールされているか否かを示す名前及びグループ、及びグラフィカルシンボルを含む。グラフィカルシンボルはルールベースマネージャ３０２とともに用いられる。

同様に、ネットワークサービス（service）はスクリーン上のブロック

３０６において定義される。これらのネットワークサービスは、ｌｏｇｉｎ、ｒｏｕｔｅ、ｓｙｓｌｏｇ、及びｔｅｌｎｅｔ等を含み得る。各サービスは、一般的な若しくは特別なプロパティによって定義される。一般的プロパティは、例えば、ｔｅｌｎｅｔ用のポート番号２３と等価な“ｄｐｏｒｔ”（デスティネートョン　ポート）のような、サービスを指定するコードストリングを含んでいる。発信するパケット及び到着するパケットを指定するこのコードストリングは内容が識別される。特別なプロパティはサービスの名称、そのサービスを提供するのに用いられるポートの名称、コネクションレスセッションが不使用の状態にあり得る秒数の制限時間、即ちそのセッションが終了したことが推定される前に何れかの方向に伝送されるパケットが存在しない状態にある秒数の制限時間を含む。サービス定義の他の要素には、受信した、ＵＤＰのようなコネクションレスプロトコルを用いるサービスに対する発信コネクション及びＲＰＣサービス用のプログラム番号が含まれ得る。グラフィックシンボル及びその色は特定される。

ブロック３０２はルールベース（rulebase）マネージャであり、これは新たなセキュリティルールをグラフィック形式でシステム内に入力できるようにする、即ちシステム管理者を、特定のセキュリティルールを実現するため、若しくはセキュリティルールの変更のためにコードを書く必要性から解放させるものである。新たなセキュリティルールをシステムに入力するために必要な要素は４つだけである。第１要素はデータパケットのソース（source）であり、第３要素はパケットのデスティネーション（destination）である。第２要素は関連するサービス（services）のタイプであり、第４要素は実行が必要なアクション（action）である。この実行され得るアクションには、パケットがソースからデスティネーションに送られる場合であるパケットの受容（accept）、若しくはソースからデスティネーションにパケットが送られない場合であるパケットの拒絶（reject）が含まれる。パケットが拒絶された場合には、何のアクションも行われないか、またはパケットがデスティネーションに届かなかったことを表す否定応

答（ＮＡＣＫ）が返送され得る。更に特定され得る別の要素は、その上でルールが施行されるオブジェクトを特定する、ルールのインストール先（install on）である（第２図参照）。インストール位置が特定されない場合には、システムはパケットフィルタモジュールを、デフォルト値である通信のデスティネーション（ＤＳＴ）上に設置する。しかし、このオブジェクトはデスティネーションである必要はない。例えば、インターネットからローカルホストに向かう通信は必ずゲートウェイを通過する。従って、ゲートウェイ（gateway）がソース、若しくはデスティネーションでない場合でも、ゲートウェイ上でルールを施行することが可能である。頭文字またはグラフィックシンボルを用いてデータを入力することによって、各ルールは即座に入力されてベリファイされ得、このとき書き込み、コンパイル及び新たなコードのチェックを行う必要は無い。従って、システム管理者は、セキュリティ用コンピュータプログラム作成の専門家である必要はない。サービスがシステムに既に入力されたサービスの１つである限り、システム管理機構のホストとしての役目を果たすコンピュータは、後に詳しく述べるように、入力された情報を処理して適当なパケットフィルタのための命令セットを生成する。

ブロック３０８はセキュリティシステムのセットアップ及び動作の概要を示すシステムステータス一覧（system status view）である。本発明を実行する必要はない。このシステム一覧は、グラフィカルシンボルを用いてシステムの概要を表示する。この概要には、例えば、ホストアイコン、ホストネーム、ルールベースを含むファイル名であるルールベースネーム、ホストにルールベースがインストールされた日付等を含まれ得る。この概要は、ホストと通信が行われたか否かということと共に、ホストによって検査され、廃棄され、及び記録されたパケット数を示すホストステータスを表示し得る。

第４図は、ＧＵＩ上の情報をパケットフィルタ用に用いられるルールを含むフィルタスクリプトに変換するサブシステムを示す流れ図である。好適実施例においては、フィルタスクリプトジェネレータの出力は、オブジェクトコードにコン

パイルされ、次いで後に説明するように、パケットフィルタモジュールによってインプリメントされる。

サブシステム４００はブロック４０２から処理を開始し、ＧＵＩからの第１ルールを含むブロック４０４に処理を進める。第１ルールは第３図に示すように、新たなセキュリティルールが特定されるスクリーン上の第１行である。次いで、制御はブロック４０６に進み、ここでルールソースネットワークオブジェクトと一致するコードが生成される。即ち、データパケットが発せられるシステムのオブジェクトの１つを表すものとしてパケットのソースがソースコートブロックに入力される。次いで、処理はブロック４０８に進み、ここでデータパケットがその行き先（デスティネーション）としているネットワークのオブジェクトを示すべく、デスティネーションコードブロックにコードが生成される。次いで、制御はブロック４１０に進み、ここで選択されたルールサービスに一致するコードが生成される。ルールサービスは以前に定義されており、システム内に格納されているか、定義されていない場合には、サービスを調整するセキュリティルールがシステムに入力されるときに定義される。次いで処理はブロック４１２に進み、ここでデータブロック４０６、４０８、及び４１０が一致しているならば、即ち、チェックの結果が真であるならば、パケットの受容若しくは拒絶を決定するコードを生成する。

受容若しくは拒絶のアクションは、セキュリティルールにおいて選択されたアクションに基づいている。次いで制御は決定ブロック４１４に進み、ここでシステムに追加的なルールを入力するか否かが決定される。システムにこれ以上のルールを入力しない場合には、サブシステムはブロック４１８で終了する。更にシステムに入力するルールが存在する場合には、処理はブロック４１６に進み、ここで新たなルールが入力されて処理はブロック４０６に戻り、プロセスが反復されてＧＵＩの次の行に示されている次のセキュリティルールが処理される。

通信プロトコルは層を成しており、これはプロトコルスタックとも称される。ＩＳＯ（国際標準化機構）は、通信プロトコル層の設定のためのフレームワークを提示する汎用モデルを定めた。このモデルは存在する通信プロトコルの機能

の理解のための基本的な参照モデルとしての役目を果たす。

ＩＳＯ　モデル

レイヤ	機　能	例
7	アプリケーション層	Ｔｅｌｎｅｔ，ＮＦＳ，ノベル社　ＮＣＰ
6	プレゼンテーション層	ＸＤＲ
5	セッション層	ＲＰＣ
4	トランスポート層	ＴＣＰ，ノベル社　ＳＰＸ
3	ネットワーク層	ＩＰ，ノベル社　ＩＰＸ
2	データリンク層（ハードウェア　インタフェース）	
1	物理層（ハードウェア　コネクション）	

通信プロトコルによって、利用するＩＳＯモデルにおけるレベルは異なる。ある層におけるプロトコルは、他の層において採用されているプロトコルに対する認識は持っていなくてもよい。これは、セキュリティアクションを作る重要な要素である。例えば、アプリケーション層（レベル７）が通信しようとするソースコンピュータ（レベル２，３）を識

別することができず、従って十分なセキュリティを提供し得なくともよい。

第５図は、本発明のフィルタパケットモジュールがＩＳＯモデル内でどのように使用されているかを示した図である。ＩＳＯモデルの通信レイヤは、第５図の左側の符号５０２で示した部分に示されている。レベル１、即ちブロック５０４はネットワークの様々なオブジェクトと接続するための線であり得るネットワークのハードウェアコネクションである。レベル２、即ち第５図のブロック５０６は、ネットワーク上の各コンピュータ内に設置されたネットワークインタフェースハードウェアである。本発明のパケットフィルタモジュールは、このレベルと、ネットワークソフトウェアであるレベル３との間に入る。構成を完成させるためＩＳＯモデルの他のレベルについて簡単に述べると、レベル４、即ちブロック５１０は１つのセグメントから次のセグメントへのデータの配送に関連し、レベル５、即ちブロック５１２はネットワーク上の“セッション”の開設及び遮断を同期させる。レベル６、即ちブロック５１４はネットワーク上の様々なコンピュ

ータの間のデータの変換に関連し、レベル７、即ちブロック５１６はアプリケーションプログラムである。

パケットフィルタモジュールが存在するコンピュータにパケットが入ってゆくとき、レイヤ１及び２を通過した後、向きを変えて第５図の右側に示すパケットフィルタ５２０に進んでゆく。このパケットはブロック５２２において受信される。ブロック５２４においては、パケットはセキュリティルールと比較され、パケットがルールに一致するものであるか否かの判定がなされる。パケットがルールに一致する場合には、システム管理機構のログにその旨が記録され、不法な試行によりシステムへの入力がなされる場合には、警告が発せられ得る。次いで、制御はブロック５３４に進み、そこでセキュリティルールの要求するところに基

づいてパケットを通過させるか否かが決定される。パケットを通過させる決定がなされた場合には、次いでパケットはレベル３、即ちブロック５０８に進む。パケットを通過させない決定がなされた場合には、ブロック５２８において否定応答（ＮＡＣＫ）が送られ、このオプションが選択された場合には、制御はブロック５３０に進み、ここでパケットが破棄、即ちそのデスティネーションに向けて通過されないことになる。同様に、アプリケーションが別のデスティネーションに送るべきパケットを生成した場合には、パケットはＩＳＯモデルのレベル３、即ちブロック５０８からブロック５２２に進み、パケットを通過させる場合にレベル３、即ちブロック５０８でなく、レベル２、即ちブロック５０６に進むことを除いて、前述のものと全く同じプロセスによって処理が進められる。次にレベル２においてパケットはネットワーク上をブロック５０４、即ちレベル１に送られる。パケットがルールに一致しない場合には、次のルールが検索され、そのパケットがこのルールに一致するか否かが検査される。デフォルトルールは特定のソース、デスティネーション、またはサービスとは無関係に任意のパケットに一致するように設けられたルールである。このｅｍｐｔｙルールのみがパケットを廃棄させるアクションを有している。一致する他のルールが存在しない場合、このルールが検索され、パケットを破棄させる効果をもたらす。パケットの破棄は

このような状況の下で取り得る最も安全なステップである。勿論、ｅｍｐｔｙルールを、パケットを通過させるように記述することもできる。

第６図を参照すると、第５図のブロック５２０が符号６００を付して詳細に示されている。第６図における一般的な表示及び第７図～第１０図に示されたより詳細な表示は、“パケットフィルタモジュール”なる用語の、ここで用いられている正確な定義を含んでいる。これらの図面

において示されている機能は、パケットフィルタモジュールを動作させるための最小限の機能である。第１１図～第１５図に示すのは、パケットフィルタモジュールに含まれ得るが、その言葉の最小限の意味においては必要ではない追加的な特徴である。

パケットフィルタモジュール“仮想マシン”として実現される。この仮想マシンは、この応用例のために、ネットワーク上のコンピュータであるホストコンピュータに存在する、第６図～第１０図に示すマシンのエミュレーションとして定義され得る。

仮想マシンは、パケットを受信するブロック６０２から処理を開始する。このブロック６０２は第５図のブロック５２２に相当する。処理はブロック６０４に進み、ここでフィルタリング操作命令が命令メモリ（図示せず）から得られる。このフィルタリング操作命令は第２図に示すパケットフィルタジェネレータ２０８によって生成されたフィルタリング操作命令である。ブロック６０４でフィルタリング操作が取り込まれた後、処理は、メモリ６１８が初期化されるブロック６０６に進む。ブロック６０８においては、第１仮想マシン操作命令が取り込まれ、ブロック６１０でそれが実行される。仮想マシンは中間値を格納するのに用いられ得るスタック若しくはレジスタ６１８のようなメモリ機構を有している。スタック若しくはレジスタの使用方法については、以下に示すテーブルに関連してより詳細に示されている。次いで処理は決定ブロック６１４に進み、ここではストップ状態に到達したか否かが判定される。ストップ状態に到達していた場合は、パケットを受容するか拒絶するかの決定がなされる。この決定はブロック６１６において実行される。パケットが通過させられた場合は、パケットは第５

図に示すように処理される。パケットが拒絶された場合は、このパケットは破棄され、ブロック５２８及び５３０において示すように否定応答（ＮＡＣＫ）が送られ

てもよい。ブロック６１４においてストップ状態に到達していない場合は、次の操作命令がブロック６１６において得られ、処理はブロック６１０から反復される。

ステップ５、即ちブロック６１０において実行され得る処理操作のタイプは、第７図においてより明確に示されている。第７図において、ブロック６１０及びブロック６１４は第６図に示したものと同一のものである。コネクション６１３に、並列に示されたこれらの処理操作が割り込んだ形となっている。ブロック６１０において行われるオペレーションに対しては、処理はそのようなタスクが実行される適当なブロック７０２、７０４、若しくは７０６に進む。ブロック７０２において、データの抽出が行われ、ブロック７０４において、論理演算が行われ、ブロック７０６において比較処理が行われる。第７図の右側に示すように、他のブロックが仮想マシンによって実行され得る処理操作と並列に追加されうる。ブロック７０２、７０４、及び７０６に示すようなサブセットは、本発明の仮想マシンにとって必要不可欠の構成要素である。これらの構成要素は第８図、第９図及び第１０図にそれぞれ詳細に示されている。仮想マシンによって実行され得る処理操作に所望に応じて含まれる追加的な構成要素は第１１図～第１５図にそれぞれ示されている。

データ抽出ブロック７０２は第８図にその詳細が示されている。このプロセスはブロック８０２から開始され、ブロック８０４に進み、そこでパケット８０６内の特定のアドレスからデータが抽出される。このアドレスは、スタックメモリ６１８、命令コードから取り込まれたものである。抽出されるデータの量もスタックメモリ、または命令コードによって決定される。抽出されたデータは、ブロック８０８においてメモリスタック８１０に入れられる。プロセスはブロック８１２で終了する。これらの図面において、制御の流れは縦方向の１直線上の矢印によって

示されているが、データの流れは右側の２本の矢印によって示されている。

第９図に示すのは、論理演算７０４の詳細である。論理演算はブロック９０２から開始され、制御はブロック９０４に進み、ここでメモリ９０６から第１値が取り込まれる。ブロック９０８において、メモリから第２値が取り込まれ、論理オペレーションはブロック９１０において実行される。論理演算の結果が真であった場合は、ブロック９１２において１がメモリ内にセットされ、論理演算の結果が偽であった場合は、ブロック９１４において０がメモリ９０６内にセットされる。プロセスはブロック９１６において終了する。

仮想マシンのための最後の、即ち第３の必須の処理操作は第１０図にその詳細が示されている。比較処理ブロック７０６はブロック１００２から開始され、制御は１００４に進み、ここでメモリ１００６から第１値が取り込まれる。制御は１００８に進み、ここでメモリ１００６から第２値が取り込まれる。第１値と第２値との間の比較処理がブロック１０１０で行われる。比較処理の結果が真であった場合には、ブロック１０１２においてメモリ１００６内に１がセットされ、比較処理の結果が偽であった場合は、ブロック１０１４においてメモリ１００６内に０がセットされる。プロセスはブロック１０１６において終了する。

以下のオペレーションは第７図には示されていないが、第７図における破線の右側に追加することができ、ブロック７０２、７０４、及び７０６と同様に、即ち並列に接続される。第１１図に示すのはメモリへのリテラル値の入力である。このプロセスはブロック１１０２から開始され、制御はブロック１１０６に進んで、ここでリテラル値が命令コードから得られる。この値はブロック１１０８においてメモリ内にセットされ、プロセスはブロック１１１０で終了する。

条件付き分岐操作が第１２図に示されている。このプロセスはブロック１２０２から開始され、制御はブロック１２０４に進み、ここで命令コードから得られた分岐条件がチェックされる。分岐条件が真であった場合は、ブロック１２０８においてメモリスタック１２０２から獲得され、ブロック１２１０においてチェックされる。ブロック１２１０における比較の結果が真であった場合には、次のステップがNにセットされ、プロセスはブロック１２１６で終了する。ブロック

１２１０における比較の結果が偽であった場合には、プロセスはブロック１２１６で終了する。分岐条件が偽であった場合には、ブロック１２０４において、処理は直接ブロック１２１４に進む。

算術演算またはビット単位の演算が第１３図に示されている。このプロセスはブロック１３０２から開始され、制御はブロック１３０４に進み、ここでメモリ１３０６から第１値が取り込まれる。第２値はブロック１３０８においてメモリ１３０６から取り込まれ、ブロック１３１０において、算術演算またはビット単位の演算がメモリ１３０６から得られた２つの値に対して施される。算術演算またはビット単位の演算の結果は、ブロック１３１２においてメモリ内にセットされ、プロセスはブロック１３１６で終了する。

セキュリティルールを実現する第１命令セットから、第２セキュリティルールのための第２命令セットにデータを送る必要がある場合に用いられる探索操作が、第１４図に示されている。第６図のブロック６０６に示すように、新たなセキュリティルールが処理される度にメモリは初期化される。従って、第１セキュリティルールによってメモリにセットされる情報を、第２セキュリティルールは使用することができない。この問題を克服するために、各ルールに対してテーブル１～３を含む個別のメモリ１４１０が与えられ、このテーブル１～３は前述の問題を克服

するために用いられ得る。テーブルへのデータの入力については第１５図に示されており、後に説明する。探索操作は１４０２から開始され、制御はブロック１４０４に進み、ここでメモリ１４０６から値が取り込まれる。制御はブロック１４０８に進み、ここで参照したテーブルで前記値を探索することによって、メモリ１４１０のテーブル１～３からデータが取り出される。制御はブロック１４１２に進み、ここでブロックがテーブル内にあるか否かが判定される。この判定の結果Ｙｅｓであれば、ブロック１４１６においてメモリ１４０６に１がセットされる。この判定の結果がＮｏであれば、ブロック１４１４においてメモリ１４０６に０がセットされる。

第１５図を参照すると、プロセスはブロック１５０２から開始され、制御は

ブロック１５０４に進み、ここでメモリ１５０６から値が取り込まれる。次いで制御はブロック１５０８に進み、ここでメモリ１５０６から取り込まれた値が、メモリ１５１０内のテーブル１～３内の適当な位置に配置される。制御はブロック１５１２に進み、ここでテーブル内への値の格納が成功したか否かに関する判定がなされる。格納が成功であった場合には、ブロック１５１６においてメモリ１５０６内に１がセットされる。格納できなかった場合には、ブロック１５１４においてメモリ１５０６内に０がセットされる。プロセスはブロック１５１８で終了する。

本発明のパケットフィルタリングメソッドを用いて実現されるセキュリティルールの一例として、システム内のＴｅｌｎｅｔサービスへのアクセスを許さないセキュリティルールの例を挙げて以下説明する。ＴｅｌｎｅｔはＴＣＰサービスであって、特定のＴＣＰデスティネーションポート番号を有するものとして定義される。これは、パケットの９バイト目の位置にＴＣＰプロトコル値６を有し、かつ、パケットの２２バイト目の位置に、２バイトのデータであるデスティネーションＴｅｌｎｅｔプロトコル番号２３を有することによって識別される。このことは全てのＴｅｌｎｅｔリクエストパケットにおいてみられることである。

以下に示す表における第１の操作は、パケットの９バイト目の位置からＩＰプロトコルを取り出し、これをメモリ内におくことである。表の右側の列の“メモリ値”に示すように、この値６はメモリスタックの最上部におかれる。

次いで第２の操作が行われる。即ち上述のＴＣＰプロトコル（ポート）番号６が、メモリ内の第２位置におかれる。第３のステップにおいて、スタックの上位の２つの層の値を比較し、結果“真”を得る。

ＴＥＬＮＥＴサービス拒絶プロセス

#	パケット フィルタコード	仮想マシン操作	メモリ値 (スタック順)		
1	pushbyte [9]	抽出操作：パケットロケーション ９からＩＰプロトコル番号を抽出し、 メモリに入れる	6		
2	push 6	メモリへのリテラル値の入力： ＴＣＰプロトコル番号をメモリに入れる	6	6	
3	eq	比較処理：ＩＰプロトコルと ＴＣＰプロトコルとを比較し、 結果“真”を得る	1		
4	pushs[22]	抽出操作：パケットロケーション ２２からＴＣＰプロトコル番号を 抽出し、メモリに入れる	1	23	
5	push 23	メモリへのリテラル値の入力： ＴＥＬＮＥＴプロトコル番号を メモリへ入れる	1	23	23
6	eq	比較処理：ＴＣＰプロトコルと ＴＥＬＮＥＴプロトコルとを比較し、 結果“真”を得る	1	1	
7	and	論理演算：ＴＣＰとＴＥＬＮＥＴの 両プロトコルが一致しているかをチェック	1		
8	btrue drop	条件付き分岐操作：メモリ値が真 (true) ならば、拒絶状態に分岐			

次いでスタックの上位２つの層における値６は消去され、結果“真”を示す値１がスタックの最上位におかれる。第４のステップにおいて、パケット上の２２バイト目の位置にあるＴＣＰプロトコル番号２３が取り出され、スタックの第２層のメモリロケーションにおかれる。第５のステップにおいてＴｅｌｎｅｔプロトコル番号のリテラル値がスタックの第３層のメモリロケーションにおかれる。第６のステップにおいて、ＴｅｌｎｅｔのＴＣＰプロトコルを含む第２、第３メモリ層のデータ値を、期待される値と比較し、結果“真”を得る。スタックの第２及び第

３の層の値は消去され、結果“真”を表す値１で置き換えられる。第７のステッ

プにおいて、ＴＣＰ及びＴｅｌｎｅｔの双方がそれぞれ一致をみたか否かを確かめるべく、論理演算が実行される。この判定はＡＮＤ演算を用いてなされる。この場合、結果は“真”であり、スタックの上位２層における値が消去されて結果“真”を示す値１で置き換えられる。第８のステップにおいて、条件付き分岐操作が実行され、このときメモリ値が真である場合は、プログラムはＴｅｌｎｅｔリクエストを通過させない破棄状態に分岐する。以上より、Ｔｅｌｎｅｔリクエストを破棄させるルールがインプリメントされたことになる。

データフローの暗号化－導入

前に述べたように、企業間、支社間、及びビジネスパートナー間での長距離通信は、最近のビジネスには欠かせないものとなった。本発明を利用することにより、インターネットのような機密保持がなされていない公衆ネットワーク上に、仮想的な私設ネットワークであるバーチャルプライベートネットワーク（ＶＰＮ）を構築することができ、これによって機密が防護され、かつ自由度の高い通信が可能となる。

発信パケットの暗号化と到着パケットの復号化、パケットへの署名、またはアドレス変換等によるパケットの変更は、パケットのフィルタモジュールによって実行される。パケットを変更するか否かの決定は、ルールベースに基づいてなされる。全てのパケットの変更、即ち暗号化、復号化、署名、及びアドレス変換は、ルールベースのコンテンツに従って選択的に実行される。例えば、暗号化が行われる場合には、ルールベース内の１つのルールが、特定のソース、デスティネーション、及びサービスの型を有するパケットに施される暗号化処理を明示的に要求しなければならない。暗号化命令はパケットフィルタリング操作記述言語に翻訳されるが、このパケットフィルタリング操作記述言語はネットワーク内の仮想パケットフィルタリングマシンにインストールされ、そこで実行される。

上述のように、パケットフィルタモジュールは、パケットを拒絶するか、受容するかを決定する。拒絶する場合には、パケットは破棄される。受容される場合には、パケットは様々な方法で変更され得る。あり得る変更の例を挙げると、

暗号化、復号化、及びアドレス変換等があるが、これらに限定されるものではない。以下、パケットフィルタモジュールによって選択的に実行されるパケットの暗号化及び復号化について詳細に説明する。

全体を通して用いられる表記

以下の表記は本明細書全体を通して使用されるものである。

記号	説明
g	全てのＤｉｆｆｉｅ－ＨｅｌｌｍａｎＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵に用いられる共通ルート
p	全てのＤｉｆｆｉｅ－ＨｅｌｌｍａｎＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵に用いられる共通モジュラス
S_{pvt}	ソース私的鍵
S_{pub}	ソース公開鍵
D_{pvt}	デスティネーション私的鍵
D_{pub}	デスティネーション公開鍵
B	ベーシック鍵
ＴＢ	短縮されたベーシック鍵
A	補助鍵
R	セッション鍵
E	セッションデータ暗号化鍵
I	セッションデータ復号化鍵
M	パケットのデータ部分
P	非暗号化パスワード
ENC_X（Y）	Ｘを鍵として用いるＹの暗号化
DCR_X（Y）	Ｘを鍵として用いるＹの復号化
ＳＩＧ（Y）	Ｙの署名

全体を通して用いられる用語の定義

以下の定義は、本発明の処理操作を理解する助けとなるものである。

用語	定義
平テキスト（平文）	暗号化されていないテキスト
クリアテキスト	暗号化されていないテキストを表す別の用語
暗号化テキスト	暗号化されたテキスト
鍵	送り手及び特定の受け手のみが知っている情報ピース
暗号化	鍵を持っていないものがメッセージを取り扱えないように、メッセージの平テキストを暗号化テキストに変換すること

復号化	メッセージの暗号化に用いられるものと同じ鍵を用いて暗号化テキストを平テキストに変換すること
認証	セキュリティを施されていない通信チャネルを通して誰でも容易に公開鍵を得られる信用ある第３者、即ち認証局（ＣＡ）が、受け取り手が確認できる公開鍵に対する証明を生成すること
電子署名	メッセージの内容そのものから生成され、メッセージ及び／若しくはその出所のデータの完全性を確認するために受け手が用いる情報
ネットワークオブジェクト	ネットワークに接続され、ネットワークとの何らかの相互作用をなすハードウェア
ゲートウェイ	少なくとも２つのネットワークに接続され、それらの間にあって情報が通過するネットワークオブジェクト
ファイヤウォールまたはファイヤウォール機能付きネットワークオブジェクト	通常ゲートウェイまたは終端ホストであるネットワークオブジェクトであって、コンピュータネットワーク上の到着及び発信データパケットフローの機密を保護するとともに、セキュリティルールベースに従ってデータパケットに選択的変更を施すネットワークオブジェクト

本発明に基づいて構成されたファイヤウォールを用いているネットワークの実施例を示す高レベルのブロック図が第１６図に示されている。図面に示されたネットワークの例は、本発明のシステムの暗号化能力を説明するために用いられるが、これは、説明のための例として取り上げたものに過ぎない。当業者は、本発明のシステムを、他のネットワークに対しても同様に適用することができよう。ホスト１及びホスト２は共に、それぞれの私設ＬＡＮに接続される。更に、ファイヤウォール１６０４がそのＬＡＮを通してホスト１に接続されており、同様にファイヤウォール２がそのＬＡＮを通してホスト２に接続される。両ファイヤウォールはインターネットのような公衆ネットワーク１６０６に接続される。また、この公衆ネットワークは機密が保護されず、信頼できないということが仮定さ

れている。認証局１（ＣＡ１）１６０２は、ホスト１及びファイヤウォール１に対する認証局（ＣＡ）として機能する。認証局２（ＣＡ２）１６１２は、ホスト２及びファイヤウォール２に対する認証局として機能する。別の実施例では、両ファイヤウォールに対して、ただ１つのＣＡが設けられる。各実施例において、ＣＡの機能は全て同様である。ただ１つの違いは、ファイヤウォールが用いるどのＣＡが公開鍵が登録されるかという点だけである。

ホスト１及びホスト２の間の通信は機密保護されることが必要である。ホスト１からの通信は、ファイヤウォール機能を備えたネットワークオブジェクトとしての役目を果たすファイヤウォール１を介して、インターネット（即ち公衆ネットワーク）にルーティングされる。同様に、ホスト２からの通信は、同様にファイヤウォール機能を備えたネットワークオブジェクトとしての役目を果たすファイヤウォール２を介して、インターネットにルーティングされる。ホスト２への通信において、ファイヤウォール１はホスト１からホスト２に向けて送られたパケットを代

行受信し（intercept）、暗号化する。ファイヤウォール２は、ホスト２に向けられて送られた暗号化されたパケットを受け取り、これらのパケットを復号化する。逆方向の通信においては、ファイヤウォール２がホスト２からホスト１に向けられたパケットを暗号化する。ファイヤウォール１は暗号化されたパケットを受信し、それらを復号化してホスト１に送る。ファイヤウォール１及びファイヤウォール２によって実行される暗号化及び復号化操作は、ホスト１及びホスト２に対して透過的である。

ホスト１がホスト２とのセッションを開設した場合、ホスト１はインターネットプロトコル（ＩＰ）パケットをホスト２に送る。ファイヤウォール１はパケットを代行受信し、ホスト１及びホスト２の間の通信が暗号化、復号化、アドレス変換等何らかの形で変更されるべきか否かを判断する。この決定は、ＩＳＯ層からの情報及び前のパケットから得て保持されていた情報に基づいて各コネクションごとに個別に行われる。この決定プロセスは、ステートフルマルチレイヤインスペクション（ＳＭＬＩ）と称される。各ファイヤウォールは、前に述べたよ

うに、ネットワークオブジェクト間の到着通信データ及び発信通信データの双方をいかに取り扱うかをファイヤウォールに指示するルールベースを保持している。ホスト１及びホスト２の間の通信は暗号化されるべきか、または電子署名されるべきかが決定された後、ファイヤウォール１は一時的にパケットを留まらせ、セッション鍵交換を開始する。これについては後に詳述する。通信の暗号化または署名が施され得る前に、両サイドは共通鍵の照合をする必要がある。この共通鍵はセッション鍵Ｒと称され、各セッションのスタート時ごとに新たなものが生成される。機密保護されていないインターネットまたは公衆ネットワークを使用することから、ファイヤウォール１とファイヤウォール２の間の通信のみが暗号化され

るということに注意されたい。ホスト１とファイヤウォール１との間の通信及びホスト２とファイヤウォール２との間の通信は、私的であって機密保護されていることが仮定され得る私設ＬＡＮ上で行われることから、暗号化されない。

セッション鍵交換－ファイヤウォール／ファイヤウォール

セッション鍵交換の間に２つのファイヤウォール間を送られるデータを示す高レベルブロック図が第１７図に示されている。以下に述べるスキームは、ＳＭＬＩを用いた暗号化処理のインプリメンテーションの一例に過ぎず、本発明の範囲はこれに限定されず、他の暗号化技術も用いられ得る。本発明の技術を実施するＳＭＬＩプロセスにおいて他の暗号化技術を利用し得るということは当業者には明らかであろう。例えば、他の実施例においてはＳＫＩＰ標準が用いられる。データの暗号化を開始するべく、ファイヤウォール１は、初めにホスト２に対してリクエストパケットを送る。このリクエストパケットは、ファイヤウォール２でなくホスト２に向けて送られるが、これはファイヤウォール１が、ホスト２を担当するファイヤウォールのＩＰアドレスを認識していないからである。リクエストパケット及び応答パケットによって、ホスト１とホスト２との間の暗号化されるべき全ての通信に対して用いられる共通鍵、即ちセッション鍵Ｒの両サイドでの照合が可能となる。前述のように、実際に暗号化されるのは、ファイヤウォール１とファイヤウォール２との間の通信のみである。

一般に、セッション鍵Rは、デスティネーションとも称される通信を仕掛けられた側のオブジェクト（即ちファイヤウォール2）１６０８によって生成され、暗号化されてソースとも称される通信を仕掛けた側のオブジェクト（即ちファイヤウォール1）１６０４に送られる。この２つのパケット交換は、暗号化された通信が開始され得る状態になる前に

行われなければならない。暗号化セッションが確立された後、状態情報は両ファイヤウォール内に保持され、ここで、留められていた元のパケットが両ファイヤウォールを暗号化されて通過させられる。ファイヤウォール２は同じセッション鍵Rを用いてホスト２からホスト１に送られるパケットを暗号化する。

ここでセッション鍵交換について詳細に説明する。共通秘密セッション鍵Rを照合するために、本発明においては、“スタティックな”ディフィー・ヘルマン・スキーム（Diffie-Hellman scheme）を用いる。各ディフィー・ヘルマン鍵は、私的部分と公開部分とを有する。両サイドは、それぞれの私的部分及び公開部分を有する。ソース（即ちファイヤウォール1）及びデスティネーション（即ちファイヤウォール2）に対する私的鍵は、それぞれＳｐｖｔ及びＤｐｖｔである。次いで、ソース及びデスティネーションの鍵の公開部分は以下のように定められる。

$$S_{pub} = g^{Spvt} \pmod{p}$$

$$D_{pub} = g^{Dpvt} \pmod{p}$$

ソース及びデスティネーションの双方は、セッション鍵交換を有効なものとするために、互いの公開鍵を知っていなければならない。一方の側が他方の公開鍵を知らない場合、若しくは有している鍵が、古いものと認められる場合には、ベーシック鍵交換が開始される。これについては後に詳述する。両サイドは互いの公開鍵を用いて、ベーシック鍵Ｂを導出する。ソースは以下の計算を行う。

$$B = \{g^{Dpvt} \pmod{p}\}^{Spvt} \pmod{p}$$

$$= g^{SpvtDpvt} \pmod{p}$$

同様に、デスティネーションは以下の計算を行う。

$$B = \{g^{Spvt} \pmod{p}\}^{Dpvt} \pmod{p}$$

$$= g^{SpvtDpvt} \pmod{p}$$

従って、両サイドはベーシック鍵Ｂを共有することになる。セッション鍵Ｒの暗号化に際して使用するときには、ベーシック鍵Ｂを短縮したものが生成され、これをＴＢと称する。

一般に、各ファイヤウォールはディフィー・ヘルマン鍵とファイヤウォール機能を備えたネットワークオブジェクトを結びつけるテーブルを保持している。更に、ファイヤウォールは、ＩＰアドレスとそのようなオブジェクトの１つとを結びつけるバインディング（binding）を有していなければならない。第１７図に示す構成においては、ファイヤウォール１内のデータベースは、ファイヤウォール２の存在を認識するように構成されていなければならない。ファイヤウォール１は、ホスト２の暗号化ファイヤウォールがファイヤウォール２であることも認識していなければならない。ファイヤウォール１は、ファイヤウォール２の暗号化ファイヤウォールとしての役目を果たしうる可能性のあるファイヤウォールのリストを有しうる。各ファイヤウォールのバインディング及びネットワークオブジェクトデータベースは、個々の管理ユニットによってスタティックに管理される。

ファイヤウォール間の通信を暗号化するために、ファイヤウォールは、それ自身のベーシック私的鍵と、それが通信する必要のある、ファイヤウォール機能を備えた各ネットワークオブジェクトのベーシック公開鍵とを知っていなければならない。ビジネスパートナーのセグメントのファイヤウォールのような、外部に存在する、ファイヤウォール機能を備えたネットワークオブジェクトのベーシック公開鍵も、暗号化セッションを開設できるようにするために知っていなければならない。このような、ベーシック鍵とファイヤウォール機能を備えたネットワークオブジェクトの間のスタティックバインディングは、ファイヤウォールの内側のデータベースに予め確立されていてもよいが、後に説明するベーシック鍵交換を用いて、通信の進行中に求めることも可能である。

共通秘密ベーシック鍵Ｂがひとたび２つのファイヤウォールによって照合さ

れると、それは、セッションに用いられる実際の鍵、即ちセッション鍵Rを暗号化するのに用いられる。同じセッション鍵Rは、ホスト１からホスト２への、あるいはホスト２からホスト１へのデータを暗号化するために、ソース及びデスティネーションの双方によって使用される。

ソースからデスティネーションへのリクエストの要素が第１７図において右向きの矢印の上に示されている。この暗号メソッドは、１または２以上の、ソースが実行可能なセッションデータの暗号化のための暗号化メソッドを含む（即ちＤＥＳ、ＦＷＺ１、ＲＣ４、ＲＣ５、ＩＤＥＡ、トリプルＤＥＳ等）。鍵メソッドは、１または２以上の、ソースが実行可能なセッション鍵Rの暗号化のための暗号化メソッドを含む（即ちＤＥＳ、ＦＷＺ１、ＲＣ４、ＲＣ５、ＩＤＥＡ、トリプルＤＥＳ等）。メッセージダイジェストメソッド（message digest method）（即ちMDメソッド）若しくはメッセージ保全メソッド（message integrity method）は、ソースが実行可能なデータ保全を実行するための１または２以上のメソッドまたはアルゴリズムを含む（即ちＭＤ５、ＳＨＡ等）。データ保全には、メッセージの一部または全ての暗号ハッシュ（cryptographic hash）の計算を伴うのが一般的である。

提案されたソース公開鍵ＩＤは、デスティネーションが使用するとソースが推定しているベーシック公開鍵を、ＩＤ番号を介して識別する。同様に、提案されたデスティネーションベーシック公開鍵ＩＤは、デスティネーションが使用するとソースが推定しているベーシック公開鍵を識別する。ホスト２を防護するファイヤウォール機能を備えたネットワークオブジェクトが複数存在する場合には、どのファイヤウォール機能を備えたネットワークオブジェクトが、実際にホスト２を防護しているかをソースが認識していないため、ソースからのリクエストパケットには、多数の提案されたベーシック公開鍵が含まれる。各提案されたベーシック公開鍵は、それぞれ異なるファイヤウォール機能を備えたネットワークオブジェクトに対応している。

このリクエストにはチャレンジ鍵Ｃも含まれており、このチャレンジ鍵Ｃは

、セッション鍵交換若しくはセッションデータそのものに対して途中で攻撃を仕掛ける妨害者の裏をかくために使用される、ソース（即ちファイヤウォール１）によって選択された任意のビットフィールドである。

デスティネーション（即ちファイヤウォール２）は、リクエストパケットを受け取り、またその内容に基づいて、ソースに送り返される応答パケットを生成する。応答パケットの要素は、第１７図における左向き矢印の上に示されている。応答パケットはリクエストパケットと類似したフォーマットを有するが、チャレンジ鍵Ｃのフィールドが、暗号化されたセッション鍵Ｒを保持するフィールドに置き換えられている点が異なっている。ここで、暗号メソッド、鍵メソッド、及びMDメソッドのそれぞれは、リクエストにあるようなオプションのリスト以外にただ１つの要素を有する。そのリストされた要素は、リクエストにおいてリストに挙げられたオプションから、デスティネーションによって選択された要素である。同様に、選択されたソースベーシック公開鍵ＩＤ及び選択されたデスティネーションベーシック公開鍵ＩＤの双方は、リクエストで送られたオプションリストからデスティネーションによって選択された鍵ＩＤを表すただ１つの鍵ＩＤを含んでいる。

応答において送られるセッション鍵Ｒは、実際には２つの鍵を含む。１つはセッションデータ暗号化鍵（session data encryption key）Ｅ、

もう１つはセッションデータ保全鍵（session data integrity key）Ｉである。従って、セッション鍵Ｒは以下のように定義される。

Ｒ＝Ｅ＋Ｉ

セッション鍵は、暗号メソッド（即ち暗号化メソッド）及びMDメソッド、またはメッセージダイジェストメソッドの双方に対して生成される任意のバイトストリームである。その長さは、暗号化メソッド及びMDメソッドによって必要とされる鍵の長さの和である。それがひとたび生成されると、MDメソッド、即ちＭＤ５によって選択され、ＳＩＧ（Ｒ）によって表されるセッション鍵の署名が得られる。セッションＲとＳＩＧ（Ｒ）の組み合わせは、次いで短縮されたベーシック鍵ＴＢ及びチャレンジ鍵Ｃの組み合わせによって形成された鍵を用いて暗号

化される。これによって、

$$ENC_{(TC+C)}(R+SIG(R))$$

が形成され、これは応答においてソースに送られる。

署名またはハッシュチェックサムの計算によって、ソースが受け取ったパケットが実際にベーシック鍵Bを認識しているエンティティによって形成されたという認証を、ソース側が得られる。従って応答パケットに対して強力な認証が与えられることになる。更に、ソースがチャレンジ鍵Cを選択することから、同じことを再度行うのは不可能である。

セッションデータ交換

セッションデータ交換中暗号化技術を用いてパケットを別のファイヤウォールに転送するときにファイヤウォールによって実行されるプロセスを示す高レベルの論理流れ図が第１８図に示されている。図面には示されていないが、別の実施例では、セッションデータ交換を実行するためにＩＰＳＥＣ標準が使用される。以前に述べたように、ソース及びデスティネーションがひとたびセッション鍵Ｒを照合すると、暗号化され

た両ファイヤウォール間の通信が進行する。パケットの代行受信及び変更は、ＩＳＯモデルのレベル２とレベル３の間で起こる。両方向の通信とも、同じセッション鍵Ｒを用いて暗号化及び復号化される。送出されるパケットは、普通のＴＣＰ／ＩＰパケットに極めて類似したものである。このパケットは、それが暗号化されているか否かを示す、あるいはその場合どの鍵が使用されるかという情報を含んでいない。この情報は、２つのファイヤウォールによって維持されている状態のなかにのみ存在する。暗号化されるトラフィックの効率及びバンド幅を増大させる役目を果たすパケットの長さの変更を行うことなく、暗号化はその場所で行われる。一般に、転送されるパケットのそれぞれは、２つの部分に分かれる。それは暗号化されないクリアテキスト部分と、暗号化される暗号化テキスト部分である。クリアテキスト部分はＩＰヘッダ及びＴＣＰ／ＵＤＰヘッダを含む。パケットの残りの部分はそのデータMを意味しており、クリアテキスト部分から算出される補助鍵Ａとセッション鍵Ｒの組み合わせを用いて暗号化される。このプ

ロセスは後に詳述する。

パケット転送時にファイヤウォールによって実行される第１ステップは、パケットそれ自体のクリアテキストの内容から補助鍵Ａを生成することである（ステップ１８００）。使用される部分は、パケットのタイプ及びプロトコルのタイプ（即ちＲＰＣ、ＵＤＰ、ＴＣＰ、ＩＣＭＰ等）に従っており、以下のようなフィールドを含み得る。即ち、例えば、ＩＰ－ＩＤ（一部分のみ）、ＲＰＣ－ＸＩＤ、ＲＰＣ－ＰＲＯＧＮＵＭ、ＴＣＰ－ＳＥＱ、ＴＣＰ－ＡＣＫ、ＵＤＰ－ＬＥＮ、ＩＣＭＰ－ＴＹＰＥ、ＩＣＭＰ－ＣＯＤＥ、及びＩＰ－ＰＲＯＴＯである。次に、補助鍵Ａ、セッションデータ保全鍵Ｉ及びパケットのデータ部分Ｍがバッファに配置される（ステップ１８０２）。次いで、ＭＤメソッドを用いてバッファのコンテンツに署名が生成され（ステップ１８０４）、それは以

下のように表される。

ＳＩＧ（Ａ＋Ｉ＋Ｍ)

生成された署名のビットは、次いでパケットヘッダにおかれる（ステップ１８０６）。パケットに署名ビットを追加することは、データの保全のために重要である。パケットの長さが変更されないことから、パケットの一部分は署名ビットで上書きされなければならない。ここでパケットが暗号化される前に署名ビットがパケット内に格納されることになる。ＴＣＰパケットの場合、２８ビットの署名が以下のように格納される。

●署名の最下位８ビットが、ＩＰ－ＩＤの最上位８ビットを置き換える。

●１の補数演算を用いて次の１６ビットがＴＣＰ－ＣＳＵＭフィールドに加えられる。

●次の４ビットが使用されないＴＣＰ－Ｘ２ニブルに格納する（これは所望に応じて行われる）。

ＵＤＰパケットに対しては、３２ビットの署名が以下のように格納される。

●署名の第１１６ビットが補数演算を用いてＵＤＰ－ＣＳＵＭフィールドに追加され、もとのＵＤＰ－ＣＳＵＭフィールドが０である場合は、同様に１の補数演算を用いてＵＤＰ－ＣＳＵＭフィールドに、ＵＤＰ－ＳＰＯＲＰ及びＵＤＰ

－ＤＰＯＲＴフィールドが追加される。

●次の１６ビットはＵＤＰ－ＬＥＮフィールドに格納される。

署名ビットがひとたびパケット内に格納されると、パケットのデータ部分Ｍは暗号化され（ステップ１８０８）、これは以下のように表される。

$$ENC_{(E+A)}(M)$$

この暗号化は、セッションデータ暗号化鍵Ｅ及び補助鍵Ａの組み合わせを用いた暗号メソッドで行われる。最後に、パケットは公衆ネットワーク上を転送される（ステップ１８１０）。

セッションデータ交換中に別のファイヤウォールからの暗号化されたパケットを受け取るときにファイヤウォールによって実行されるプロセスを示す高レベルの論理流れ図が第１９図に示されている。初めに、署名を認証するために、補助鍵Ａがパケットの内容から生成されなければならない（ステップ１９００）。次いで、パケットのデータ部分Ｍが暗号メソッド及びセッションデータ暗号化鍵Ｅ及び補助鍵Ａの組み合わせを用いて復号化される（ステップ１９０２）。これは以下のように表される。

$$DCR_{(E+A)}(ENC_{(E+A)}(M))$$

次に、署名ビットがパケットヘッダから抽出される（ステップ１９０４）。次いで、補助鍵Ａ上の署名、セッションデータ保全鍵Ｉ及びパケットデータＭがＭＤメソッドを用いて生成される（ステップ１９０６）。これは以下のように表される。

$$SIG(A+I+M)$$

次いで２つの署名が互いに比較される（ステップ１９０８）。署名が一致した場合は、署名データを上書きされたパケットに対して何らかのデータの置き換えが行われた後、パケットが送られる（ステップ１９１０）。署名が一致しない場合は、パケットは破棄される（ステップ１９１２）。

ベーシック鍵交換

前に説明したように、ファイヤウォールを備えたネットワークオブジェクトの間の通信を暗号化するために、ファイヤウォールはそれ自身の私的ベーシック

鍵及びそれが通信する必要のある各ファイヤウォールの公開ベーシック鍵を認識していなければならない。ビジネスパートナー

に属するファイヤウォールのような外部ファイヤウォールに属する公開ベーシック鍵も、暗号化されたセッションの生成のために認識されなければならない。ベーシック鍵とファイヤウォールらのスタティックな結合は、データベース内においてファイヤウォールに対して既に確立されているはずであり、若しくはベーシック鍵交換を用いて処理の進行中に成立させることができる。更に、ベーシック鍵はセキュリティーを改善するために、随時変更されてもよい。本発明においては、ベーシック公開鍵がファイヤウォール内部のデータベース内に既に存在しない場合は、ベーシック公開鍵を処理進行中に得ることができる。一般に、デスティネーションのベーシック公開鍵をソースが認識していない場合、若しくはソースによって使用されるデスティネーションベーシック公開鍵が古いものであると認められた場合には、ベーシック公開鍵が得られなければならない。

何れの場合においても、ベーシック公開鍵の交換は、転送されるディフィー・ヘルマン鍵の認証を確保するために検証される。一般にメッセージの検証により、システムに対し途中で攻撃を仕掛ける妨害者の裏をかくことができる。

ベーシック鍵を交換するプロセスを以下に詳しく説明する。ベーシック鍵交換中に２つのファイヤウォール間で転送されるデータを示した高レベルのブロック図が第２０図に示されている。両サイドの何れかがその通信相手（peer）のための有効鍵を有していない場合か、古くなった鍵を有していない場合か、古くなった鍵を有していることを認識した場合には常に、認証されたベーシック鍵を送るように他の側にリクエストを行う。

ベーシック鍵交換の開始のしかたには、ベーシック公開鍵が更新若しくは交換されなければならないということをどちらの側が認識したかに

よって決まる２つの方式があり得る。典型的には、他方のベーシック鍵を有していない側がそのことを認識する。例えば、第１６図を参照すると、開始側、即ちファイヤウォール１が、ファイヤウォール２に対するベーシック公開鍵を有して

いないことを認識した場合には、そこでベーシック鍵交換が開始される。別のシナリオでは、ファイヤウォール２がファイヤウォール１からのリクエストを受け取ったとき、ファイヤウォール１に対するベーシック公開鍵の古いバージョンを有していることを確認する（これはリクエストにおいて送られた、提案されたベーシック公開鍵とデータベース内のデータを比較することによって行われる）。後者のシナリオの一例が第２０図に示されている。

ベーシック鍵リクエストの要素は、第２０図の左向き矢印の上に示されている。ベーシックリクエストは、ソースベーシック公開鍵ＩＤ、デスティネーションベーシック公開鍵ＩＤ、暗号メソッド、鍵メソッド、及びMDメソッドを含む。これらの要素は、本明細書のセッション鍵交換－ファイヤウォール／ファイヤウォールと題されたセクションにおいて上述したものと同一のものである。ベーシック鍵交換が起こらなければならないときには、認証された鍵更新または鍵ｓｙｎｃを他方に送る側が、リクエストにＣＡ公開鍵ＩＤフィールドを追加する。この新たなフィールドはどの鍵が更新を要求しているかを示し、それによってファイヤウォール２がファイヤウォール１からの応答を受け取ることを要求する認証局（ＣＡ）鍵（即ちＲＳＡ鍵）のＩＤである。このメッセージを受け取ったとき、ファイヤウォール１はそのベーシック公開鍵Ｓｐｕｂをファイヤウォール２に送るが、その前にＣＡ公開鍵と共にＣＡによってなされる認証を受ける。認証はベーシック公開鍵の電子署名を生成するプロセスである。ファイヤウォール１に対しては、ＣＡ１（１６０２）が、ファイヤウォール１のベーシック公開鍵（第１６図）を確認す

るためのＣＡ公開鍵を生成する。ファイヤウォール２が署名の確認を行うために、ＣＡ１、即ちファイヤウォール１用の認証局（ＣＡ）からのＣＡ公開鍵を受け取らなければならない。

ファイヤウォール１による応答の要素は、第２０図の右向き矢印の上に示されている。この要素はＣＡ公開鍵ＩＤ、ソースベーシック公開鍵Ｓｐｕｂ及びＩＰアドレスまたはソースアドレスを含んでいる。更に、ソースベーシック公開鍵の署名が送られるが、これは以下のように表される。

$SIG(S_{pub})$

好適実施例においては、この署名の生成過程では、初めに、電子署名を生成するMDメソッドを用いて、送られるべきベーシック公開鍵から中間的署名を生成する。次いで、最終的に転送される署名を生成するべく、この中間的署名がＲＳＡ復号化関数に入力される。ソース（即ちファイヤウォール１）のＩＰアドレスは、そのファイヤウォール、即ちファイヤウォール１とベーシック公開鍵（Ｓｐｕｂ）との間のバインド（連結）を確認するために含まれている。

ファイヤウォール１からの認証を受け取ったとき、ファイヤウォール２はＣＡ公開鍵を用いてそれを確認することができる。正しいと確認された場合には、ファイヤウォール２は、そのデータベースをファイヤウォール１の新たなベーシック公開鍵に更新する。ここで、セッション鍵交換が完了し、セッションデータの通信が行われ得ることになる。

ここで、ベーシック公開鍵が、各ファイヤウォールとそのＣＡとの間を機密保持された通信チャネルを介して通信されることに注意されたい。１または２以上のＣＡが存在する場合には、１つのＣＡの公開鍵は他のＣＡに妨げられることなく送られる。このメッセージは、ＣＡ公開鍵の以前の値を用いて署名されるか、あるいは新たに得られたＣＡ公開鍵が

ＦＡＸまたは電話等のマニュアルな手段を用いて確認され得る。

セッション鍵交換－クライアント／ファイヤウォール

以前に説明したように、ビジネス上、企業ネットワークへの外部からのアクセスの必要性が高まってきている。会社のＬＡＮまたはＷＡＮ環境から物理的外部で働いているが、それに接続する必要のある社員の数も増加している。本発明により、システムの外部ユーザを確認することが可能となり、外部ユーザ若しくはクライアントとホストシステムとの間の暗号化された通信が可能となる。

本発明に基づいて構築されたファイヤウォール及びクライアントパーソナルコンピュータを備えた構成の例を示す高レベルのブロック図が第２１図に示されている。パーソナルコンピュータ（ＰＣ）２１００は、説明の便宜上ここではリソースと称され、クライアントまたは外部ユーザがＬＡＮに接続されたホスト２１

０４のログインするのに使用される。このＰＣは公衆ネットワーク１６０６に接続されており、ファイヤウォール２１０２を介して、説明の便宜上サーバまたはデスティネーションと称されるホストと通信を行う。ＰＣとホストとの間の全ての通信は、ファイヤウォールを通してなされる。このＰＣはホストにログインし、それとファイヤウォールとの間の暗号化通信を実行するのに必要な機能を発揮するべく適切にプログラムがなされている。第１６図に示されている構成と同様に、第２１図の構成においても、暗号化通信はＰＣとファイヤウォールとの間でのみ行われる。ホストに対しては、ファイヤウォールは透過的であり、データがＰＣから直接入ってくるものとみなすことができる。

ファイヤウォールに対するクライアント用のセッションデータ交換プロセスは、ファイヤウォールに対するファイヤウォールのそれに類似している。しかし、セッション鍵交換及びベーシック鍵交換プロセスに異

なる点がある。ファイヤウォールーファイヤウォールセッション鍵交換においては、各セッションが異なるセッション鍵を受信していた。セッションは、２つの特定のネットワークオブジェクト間のコネクションであるのみならず、同じネットワークオブジェクト間の異なるサービスの間のコネクションを含み得る。これに対し、クライアントはホストとのセッション及びクライアントがリクエストした動作若しくはサービスがいかなるものであれ、同じ鍵を用いてセッションが暗号化されるときに、クライアントとホストの間の全ての通信を初期化する。更に、ファイヤウォール間の通信においては、両サイドが互いの認証公開鍵を有していた。クライアントとファイヤウォール間の通信においては、このことはクライアントに対してのみ当てはまり、サーバはクライアントが送るネーム／パスワードのデータ対を用いてクライアントを識別する。

セッション鍵交換中のクライアントパーソナルコンピュータとファイヤウォール間のデータ転送を示す高レベルブロック図が、第２２図に示されている。クライアントによるリクエストにおいて送られた要素は、右向きの矢印の上に示されている。この要素は、名前（name）、暗号メソッド、鍵メソッド、MDメソッド、パスワードメソッド、ソースベーシック公開鍵Ｓｐｕｂ、提案されたデスティ

ネーションベーシック公開鍵ＩＤ、チャレンジ鍵Ｃ、暗号化されたパスワード及び署名を含んでいる。名前は、クライアントを現在用いているユーザを識別するのに用いられる。暗号メソッド、鍵メソッド及びMDメソッドについては以前に説明した。パスワードメソッドは、パスワードの暗号化に際してどの暗号メソッドを用いるかを示す。暗号化されたパスワードは以下のように表され得る。

$$ENC_{(TB+C)}(P)$$

ソースベーシック公開鍵Ｓｐｕｂは、ファイヤウォールがユーザのリスト及びそれに関連するベーシック公開鍵を保持していない時は常に送られる。送られるデータは、本明細書のベーシック鍵交換－ファイヤウォール／ファイヤウォールなる表題のセクションで説明したように、ファイヤウォール１からファイヤウォール２（第２０図）に送られるデータに類似したものである。デスティネーションベーシック公開鍵ＩＤは、本明細書のセッション鍵交換－ファイヤウォール／ファイヤウォールなる表題のセクションで説明したのと同一のものである。

署名はデスティネーション、即ち受け取り側に対してメッセージが変更されなかったことを確認する役目を果たす。この署名は、第２２図においてＴで表されているリクエストまたはメッセージの全内容のうち、署名フィールドを除く全内容を取り出し、Ｔと暗号化されていないパスワード及び短縮されたベーシック公開鍵ＴＢを結びつけることによって生成され、以下のように表される。

$$SIG(T+P+TB)$$

この署名はリクエストに追加され、次いでこのリクエストはファイヤウォールに送られる。

リクエストが受け取られた後、ファイヤウォールは、クライアントのソースベーシック公開鍵Ｓｐｕｂを認識する。ここで、ベーシック鍵Ｂ及び短縮されたベーシック鍵ＴＢの生成が可能となる。次いで、パスワードＰの暗号化が可能となる。ひとたびＰが認識されると、ファイヤウォールはリクエスト内の署名を確認することができる。次に、ファイヤウォールはクライアントからのリクエストにおいて送られたチャレンジ鍵Ｃ及び短縮されたベーシック鍵ＴＢを用いて、任

意のセッション鍵R及びRの署名を生成してそれを暗号化する。これを式で表すと以下のようになる。

$$ENC_{(TB+C)}\ (R+SIG\ (R))$$

次いで、署名が、第２２図においてUで示されたリクエストの内容と共に、短縮されたベーシック鍵ＴＢから生成される。これを式で表すと以下のようになる。

$$SIG\ (U+TB)$$

次いでファイヤウォールは、その要素が第２２図の左向き矢印の上に示されている応答を生成する。この応答はデスティネーションベーシック公開鍵ＩＤ、暗号メソッド、鍵メソッド及びMDメソッド、暗号化されたセッション鍵及び署名を含む。

セッション鍵がクライアントとファイヤウォールの双方によってひとたび認識されると、ファイヤウォールを介してのＰＣとホストの間の通信セッションを進めることができるようになり、ＰＣとファイヤウォールとの間の暗号化通信はホストに対して透過的となる。鍵交換の数を減らすために、セッション鍵Rは同じファイヤウォールを通る全ての暗号化コネクションに対して用いられる。所定の時間の経過後、即ち数分間の経過後、セッション鍵Rは破棄される。

ベーシック鍵交換ークライアント／ファイヤウオール

ファイヤウォールとファイヤウォールとの間の通信とは異なり、認証された鍵の交換は、ファイヤウォールのベーシック公開鍵でクライアントを更新するためにのみ必要である。ベーシック鍵交換開始には２つの場合があり得る。その１つはクライアントがファイヤウォールベーシック公開鍵を有していない場合、もう１つはファイヤウォールが、リクエストに際してクライアントによって使用されるベーシック公開鍵が古くなっていることを確認した場合である。

このプロセスは、以前にベーシック鍵交換ーファイヤウォール／ファイヤウォールなる表題のセクションで説明したようなベーシック鍵交換に類似したものである。しかし、以下のような相違点がある。クライア

ントがファイヤウォールのベーシック公開鍵を有していないことを認識した場合

、リクエストにおけるデスティネーションベーシック公開鍵ＩＤフィールドの代わりにＣＡ公開鍵ＩＤフィールドを用いる。このことは第２３図の右向き矢印の上に示されている。第２３図は、ベーシック鍵交換中のクライアントパーソナルコンピュータとファイヤウォールとの間のデータ転送を示す高レベルのブロック図である。この鍵ＩＤは、ファイヤウォールからの応答を受け取ることを要求しているクライアントによる認証局（ＣＡ）鍵（即ちＲＳＡ鍵）のＩＤである。

ファイヤウォールは、クライアントからリクエストを受け取ったとき、リクエストを元に、クライアントがファイヤウォールのベーシック公開鍵をリクエストしているのか、リクエストにおける鍵ＩＤがファイヤウォールのベーシック公開鍵と一致していないか否かを判定する。ファイヤウォールの応答の要素は、図面の左向き矢印の上に示されている。この応答は、元の提案されたデスティネーションベーシック公開鍵ＩＤ、ＣＡ公開鍵ＩＤ、デスティネーションベーシック公開鍵Ｄｐｕｂ、デスティネーションのアドレス、及び署名を有している。元のデスティネーションベーシック公開鍵は、デスティネーションからの場合と同様に取り出される。デスティネーションベーシック公開鍵の署名が送られるが、この署名を式で表すと以下のようになる。

$$SIG(D_{pub})$$

好適実施例において、この署名の生成は、電子署名を生成するMDメソッドを用いて、送られたベーシック公開鍵から中間的署名を生成することによってなされる。次いで、この中間的署名は、最終的に転送される署名を生成するべくＲＳＡ復号化機構に入力される。デスティネーション（即ちファイヤウォール）のＩＰアドレスは、ファイヤウォールとベーシック公開鍵Ｄｐｕｂとの間のバインドを確認するために含まれて

いる。

ファイヤウォールからの認証のためのデータを受け取ったとき、クライアントはＣＡ公開鍵を用いてそれを認証することができる。それが正しいと認証された場合には、クライアントはそのデータベースをファイヤウォールの新たな公開鍵で更新する。

ファイヤウォールの応答を受け取った後、クライアントはメッセージを送り返して認証を完了する。メッセージの要素は、第２３図の下側の右向き矢印の上に示されている。このメッセージには、暗号化されたパスワード及び署名が含まれている。応答がひとたび受け取られると、クライアントはベーシック鍵Ｂ及び短縮されたベーシック鍵ＴＢを生成することができる。次いでクライアントはパスワードＰを暗号化し、これを式で表すと以下のようになる。

$$ENC_{(TB+c)}(P)$$

この署名は第２２図における右向き矢印の上に示されたような、ファイヤウォールに送られる元のリクエスト（Ｔとして表されている）と、クリアテキストパスワードＰ、及び短縮されたベーシックキーＴＢの組み合わせを元にして、ＭＤメソッドを用いて生成され、これを式で表すと以下のようになる。

$$SIG(T+P+TB)$$

次いで、暗号化されたパスワード及び署名がファイヤウォールに送られる。こうしてセッションキー交換が完了し、セッションデータ通信が開始できるようになる。

本発明のいくつかの実施例について以上説明してきたが、その様々な変更、改良、及び別の形態の応用が可能であることは明らかであろう。

【図１】

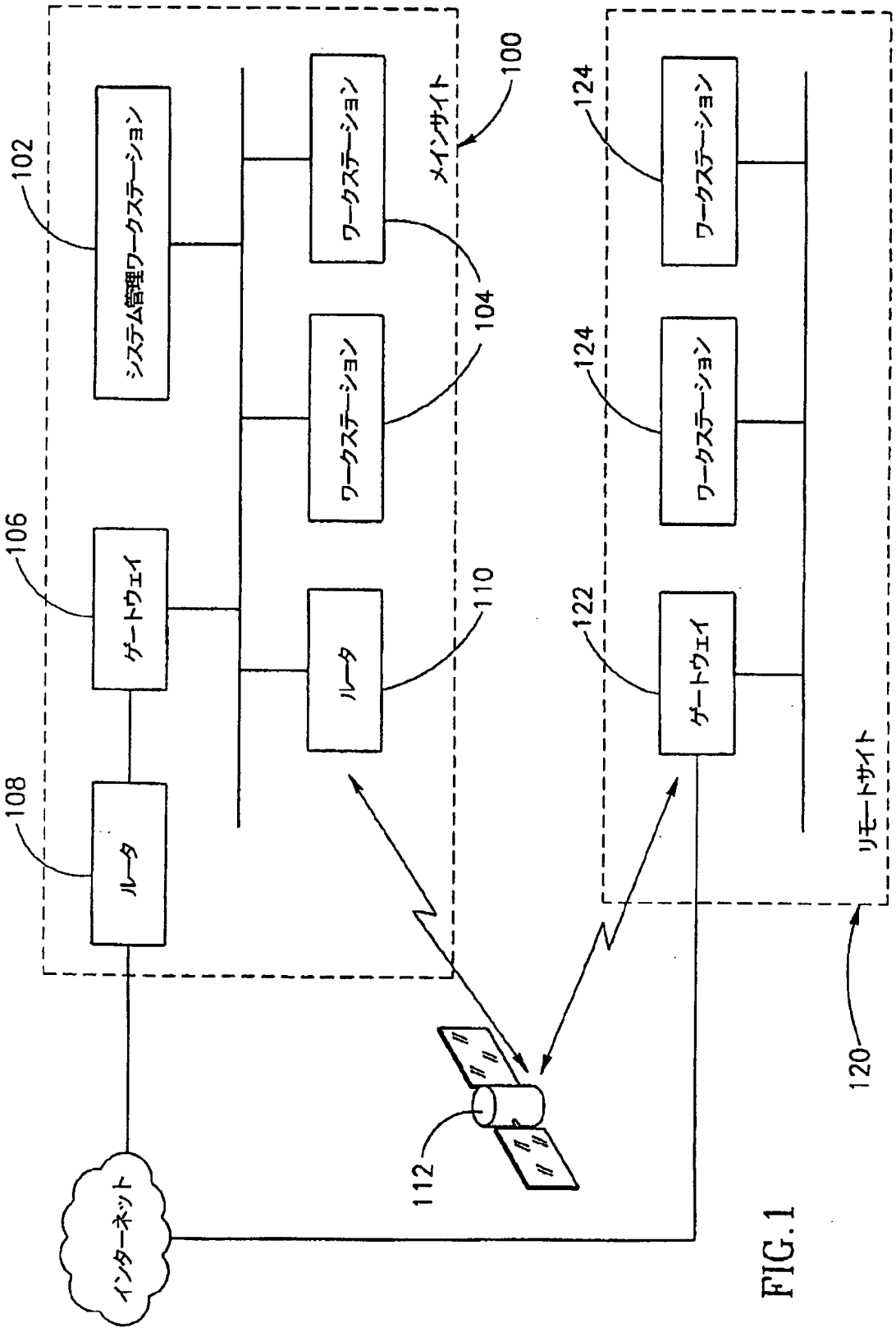

メインサイト
100
システム管理ワークステーション
102
ワークステーション
104
ゲートウェイ
106
ルータ
108
ルータ
110
インターネット
112
ワークステーション
124
ワークステーション
124
ゲートウェイ
122
リモートサイト
120

FIG. 1

【図２】

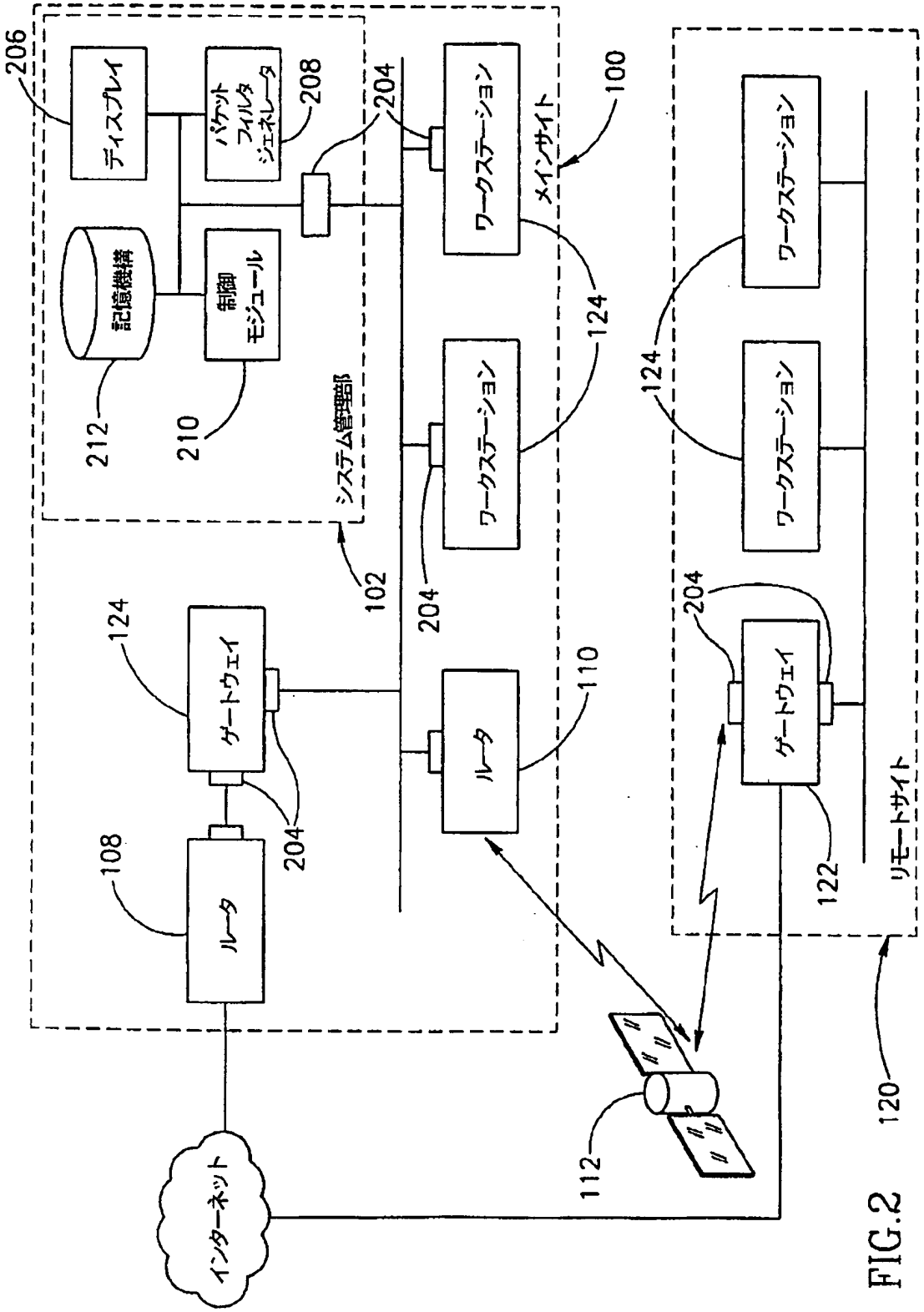

206
ディスプレイ
パケットフィルタジェネレータ
208
204
ワークステーション
メインサイト
100
記憶機構
制御モジュール
212
210
システム管理部
102
124
ワークステーション
ワークステーション
204
124
ゲートウェイ
ルータ
110
108
ルータ
204
ゲートウェイ
204
ワークステーション
ワークステーション
124
122
リモートサイト
120
112
インターネット

FIG.2

【図３】

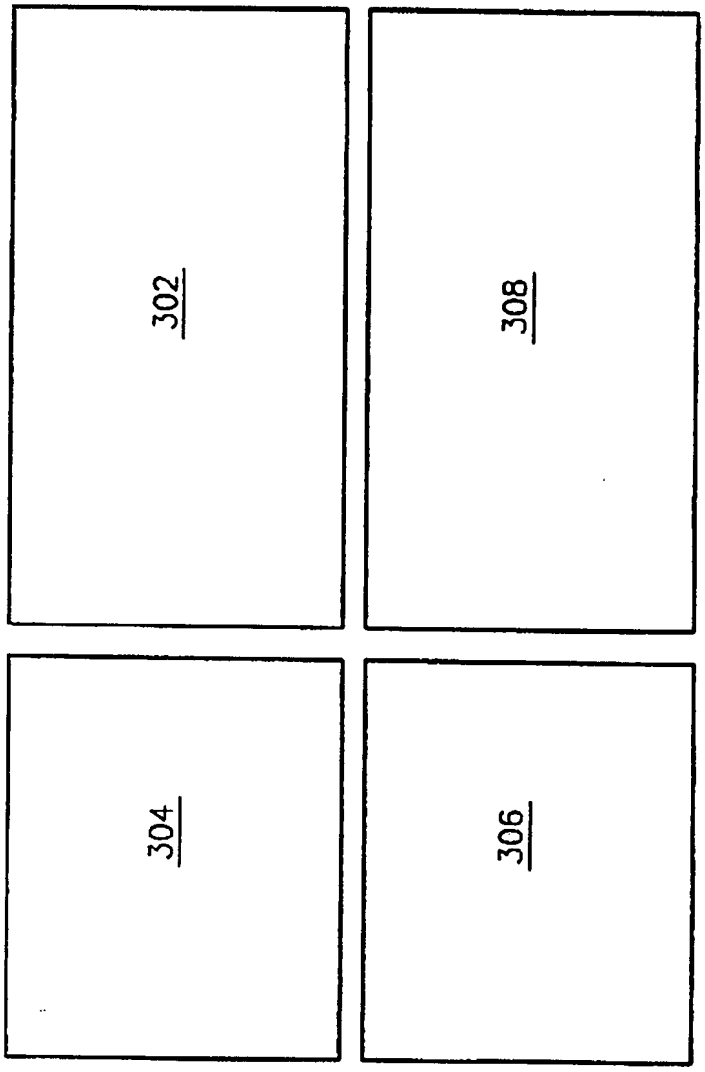


FIG.3/1

【図3】

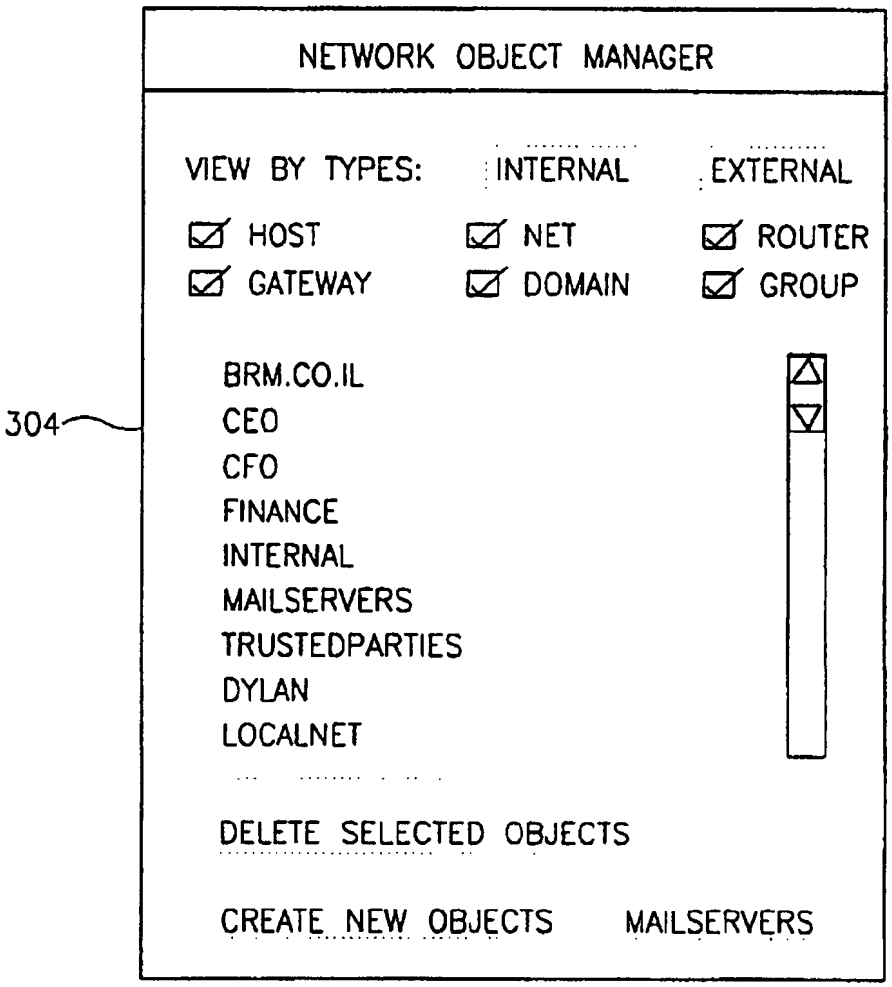

NETWORK OBJECT MANAGER
VIEW BY TYPES:
INTERNAL
EXTERNAL
HOST
NET
ROUTER
GATEWAY
DOMAIN
GROUP
304
BRM.CO.IL
CEO
CFO
FINANCE
INTERNAL
MAILSERVERS
TRUSTEDPARTIES
DYLAN
LOCALNET
DELETE SELECTED OBJECTS
CREATE NEW OBJECTS
MAILSERVERS

FIG.3/2

【図３】

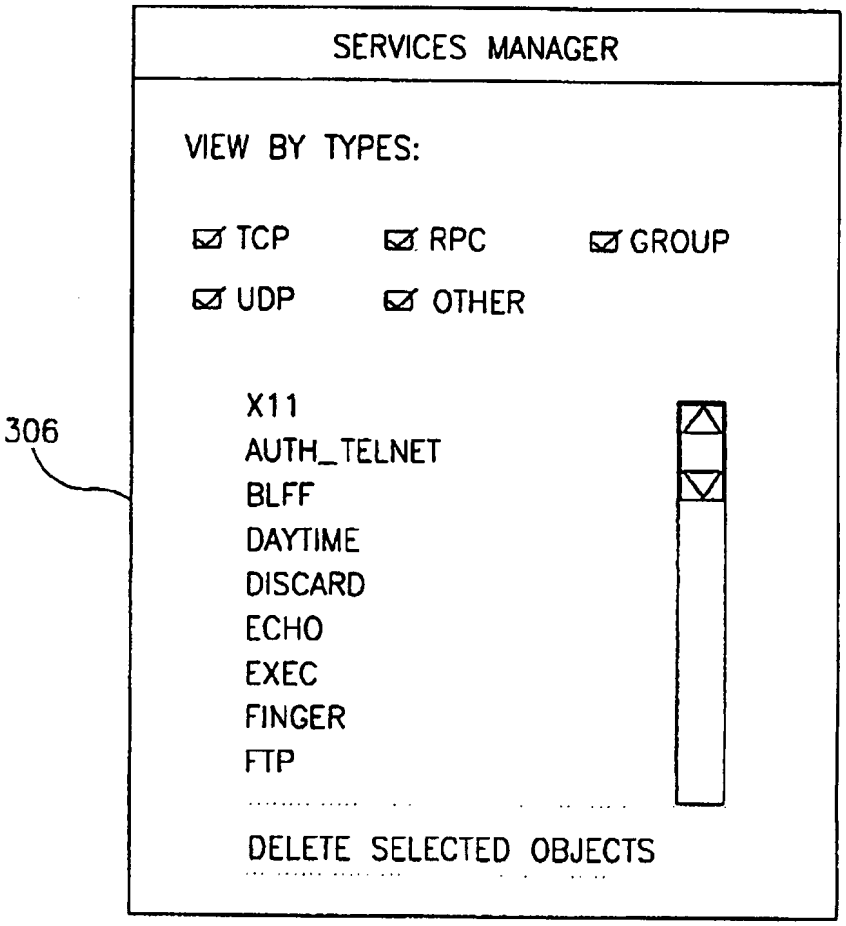

SERVICES MANAGER
VIEW BY TYPES:
TCP
RPC
GROUP
UDP
OTHER
306
X11
AUTH_TELNET
BLFF
DAYTIME
DISCARD
ECHO
EXEC
FINGER
FTP
DELETE SELECTED OBJECTS

FIG.3/3

RULE BASE EDITOR : CORPORATE

FILE | RULE | FILTER | ROUTER | UTILITES | PROPERTIES | TUTORIAL

WINDOWS: ☑ NETWORK OBJECTS ☑ SERVICES ☑ SYSTEM VIEW ☐ LOG VIEWER

NO.	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	INSTALL ON
1	ANY	MAILSERVERS	SMTP	ACCEPT		GATEWAYS GW
2	☐ CEO ☐ CFO	FINANCE	ANY	DROP STOP	ALERT	GATEWAYS GW
3	TRUSTEDPARTIES	INTERNAL	TALK RSTAT TELNET	ACCEPT		DST
4	INTERNAL	ANY	ANY	ACCEPT	ALERT	GATEWAYS GW
5	ANY	INTERNAL FINANCE	ANY	REJECT STOP	MAIL	DST

RULE BASE SAVED TO '/FW/USERS/MARLUS/CORPORATE.W'

FIG.3/4

302

【図3】

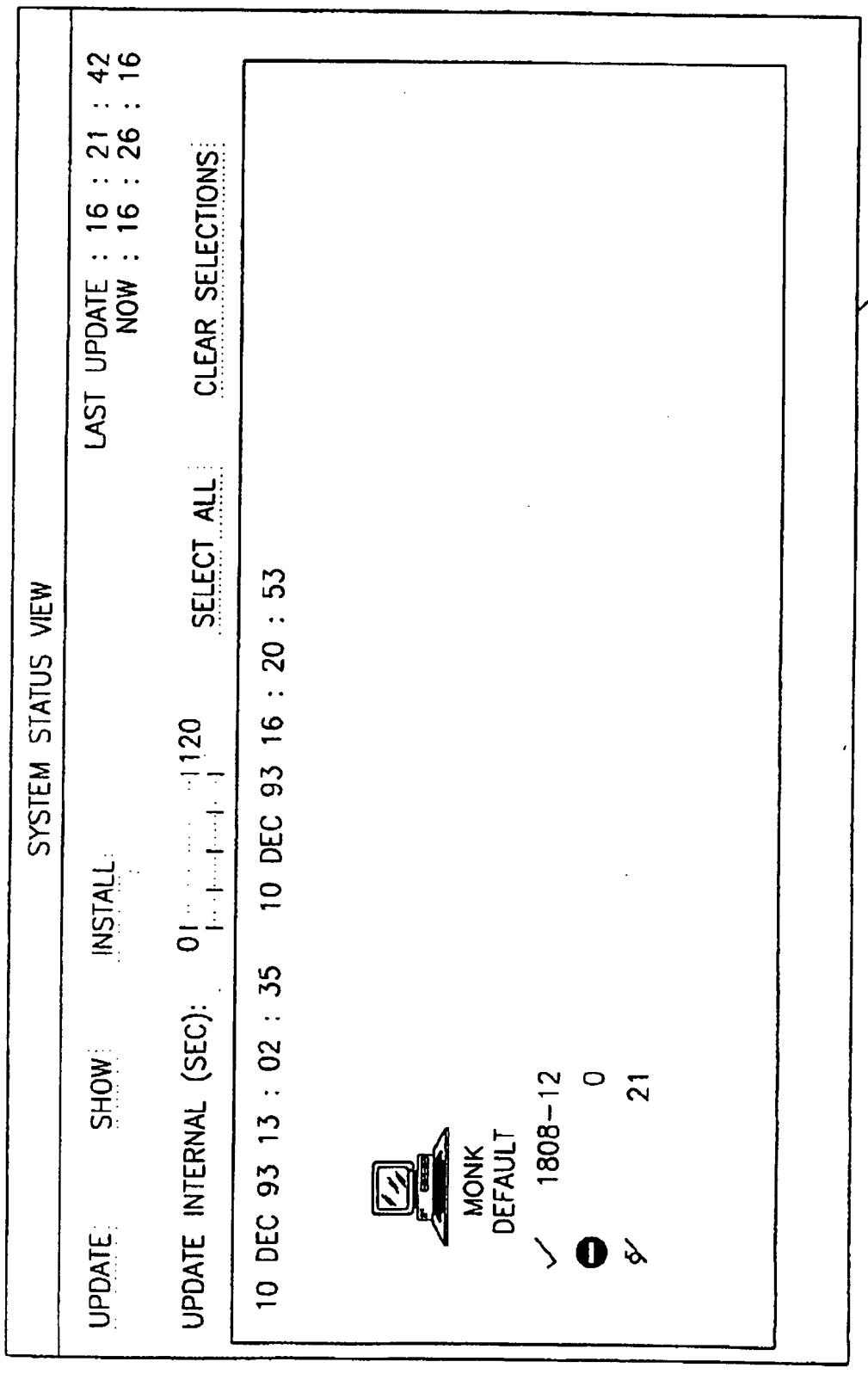

SYSTEM STATUS VIEW
UPDATE
SHOW
INSTALL
LAST UPDATE : 16 : 21 : 42
NOW : 16 : 26 : 16
UPDATE INTERNAL (SEC): 0 1 120
SELECT ALL
CLEAR SELECTIONS
10 DEC 93 13 : 02 : 35
10 DEC 93 16 : 20 : 53
MONK
DEFAULT
1808-12
0
21
308

FIG.3/5

【図４】

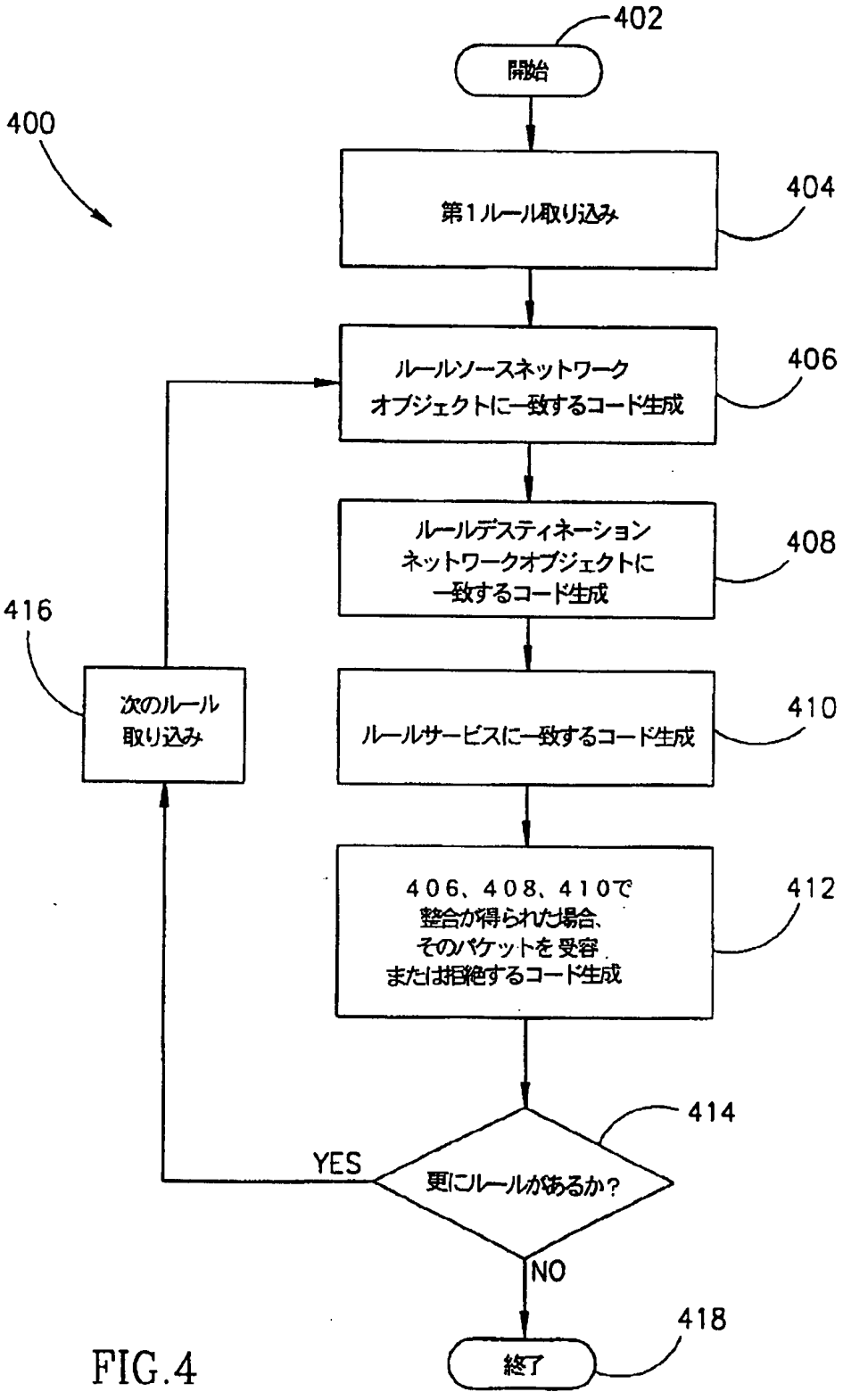

402
開始
400
第1ルール取り込み
404
ルールソースネットワーク
オブジェクトに一致するコード生成
406
ルールデスティネーション
ネットワークオブジェクトに
一致するコード生成
408
416
次のルール
取り込み
ルールサービスに一致するコード生成
410
406、408、410で
整合が得られた場合、
そのパケットを受容
または拒絶するコード生成
412
414
YES
更にルールがあるか？
NO
418
終了

FIG.4

【図5】

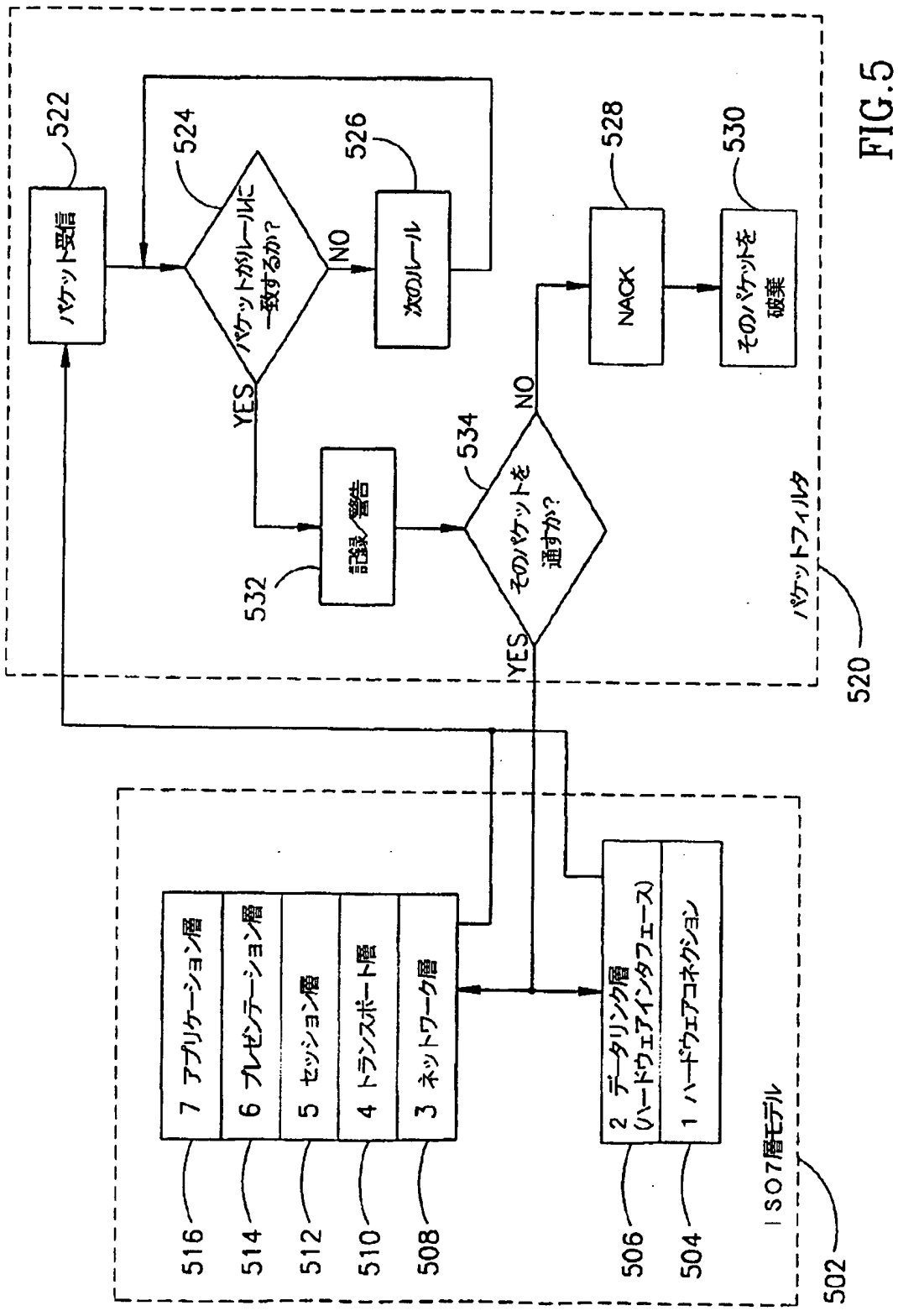

パケットフィルタ
520
パケット受信
522
パケットがルールに一致するか？
524
YES
NO
次のルール
526
記録／警告
532
そのパケットを通すか？
534
YES
NO
NACK
528
そのパケットを破棄
530
ISO7層モデル
502
7 アプリケーション層
6 プレゼンテーション層
5 セッション層
4 トランスポート層
3 ネットワーク層
2 データリンク層（ハードウェアインタフェース）
1 ハードウェアコネクション
516
514
512
510
508
506
504

FIG.5

【図６】

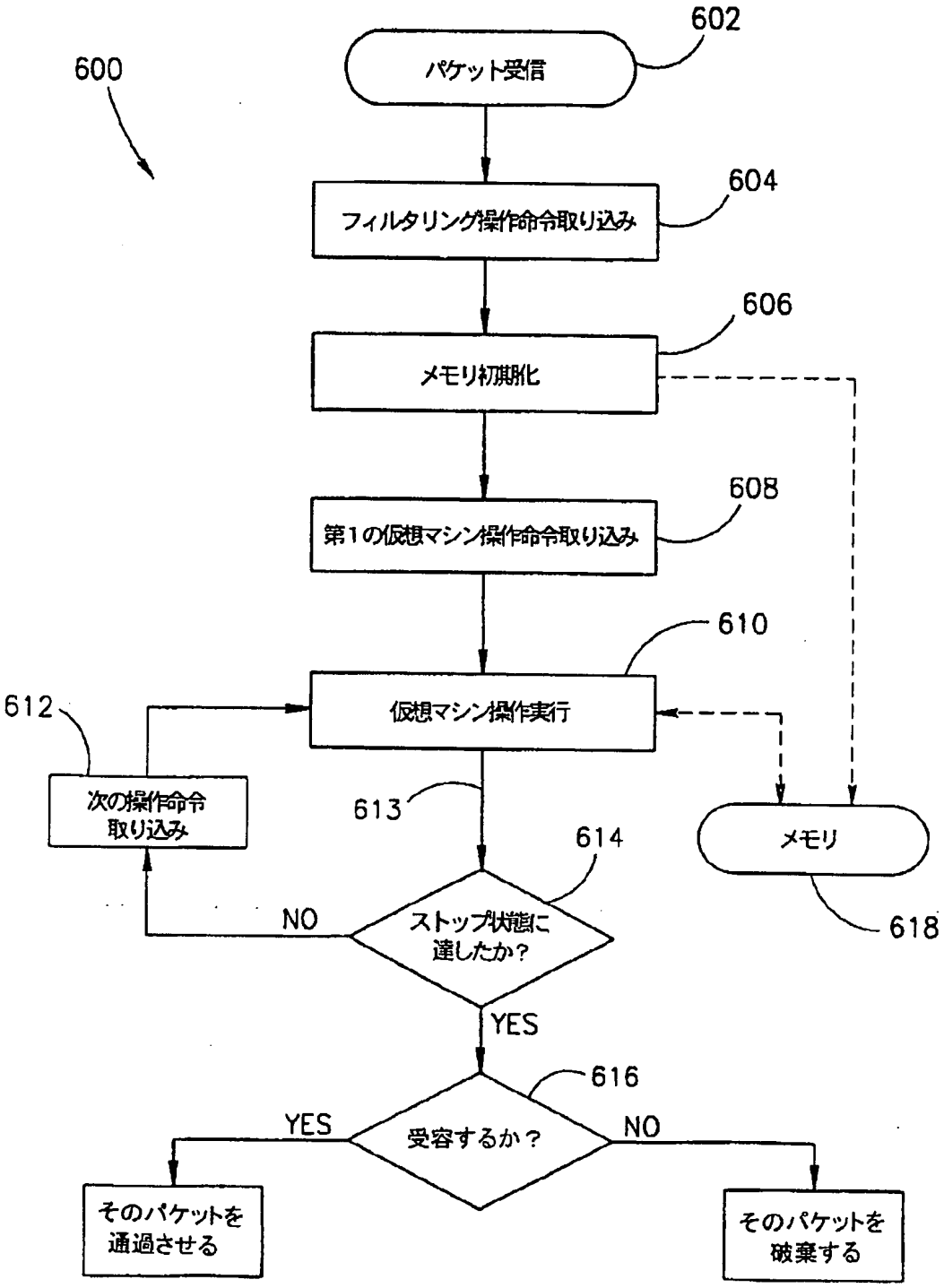

600
602
パケット受信
604
フィルタリング操作命令取り込み
606
メモリ初期化
608
第１の仮想マシン操作命令取り込み
610
仮想マシン操作実行
612
次の操作命令
取り込み
613
614
ストップ状態に
達したか？
NO
YES
616
受容するか？
YES
NO
そのパケットを
通過させる
そのパケットを
破棄する
メモリ
618

FIG.6

【図７】

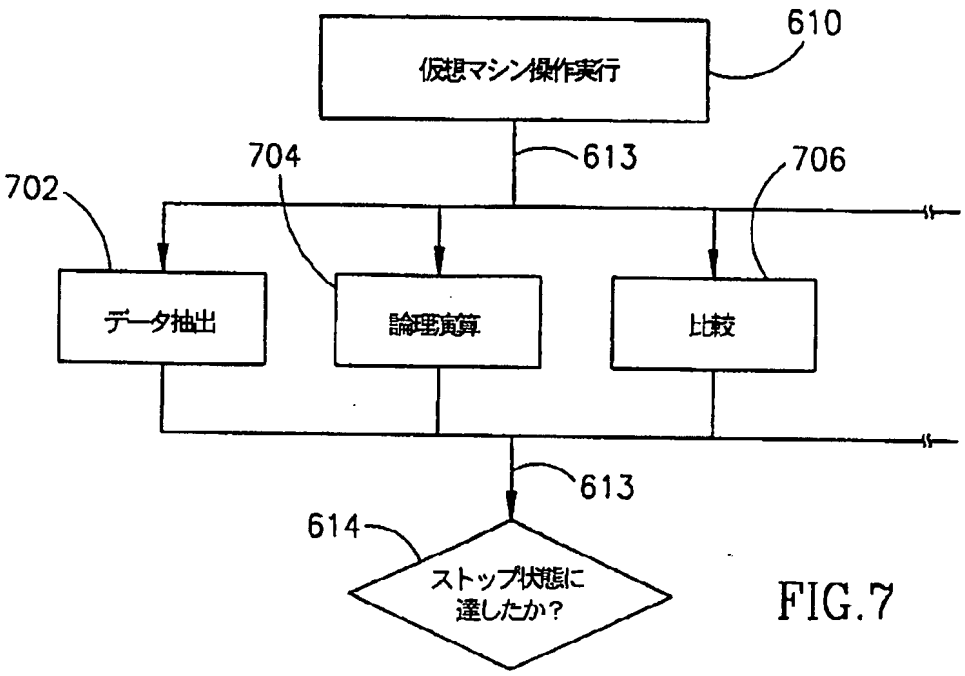


FIG.7

【図８】

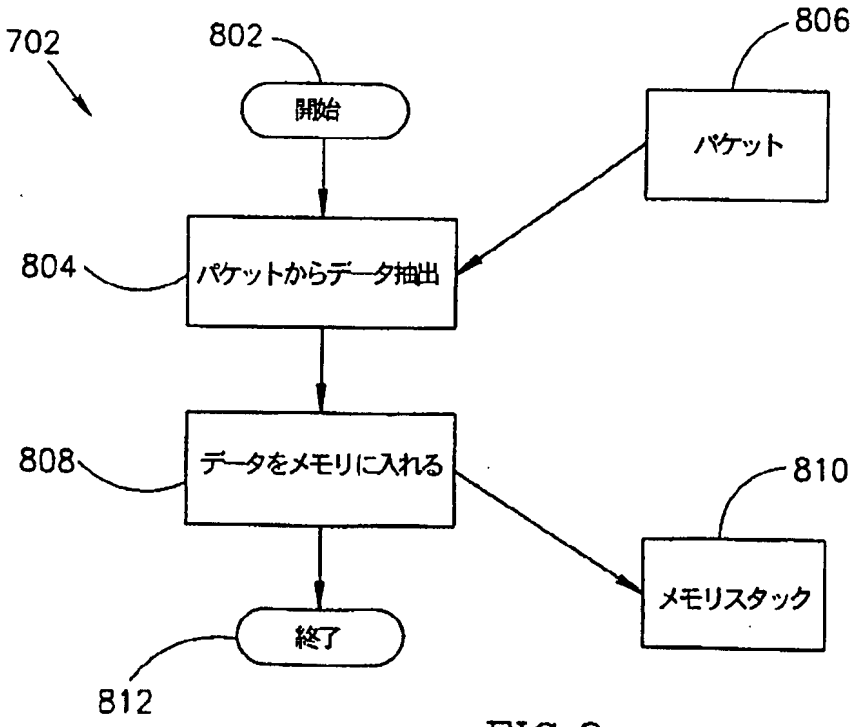


FIG.8

【図９】

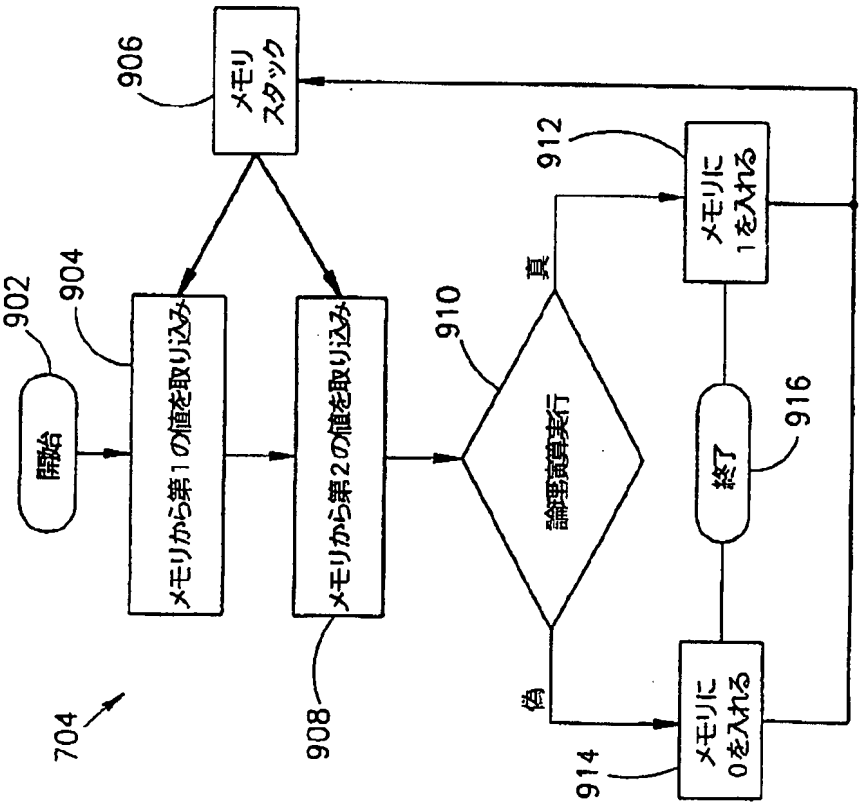

704
902
開始
904
メモリから第1の値を取り込み
908
メモリから第2の値を取り込み
910
論理演算実行
真
912
メモリに1を入れる
偽
914
メモリに0を入れる
916
終了
906
メモリスタック

FIG.9

【図１０】

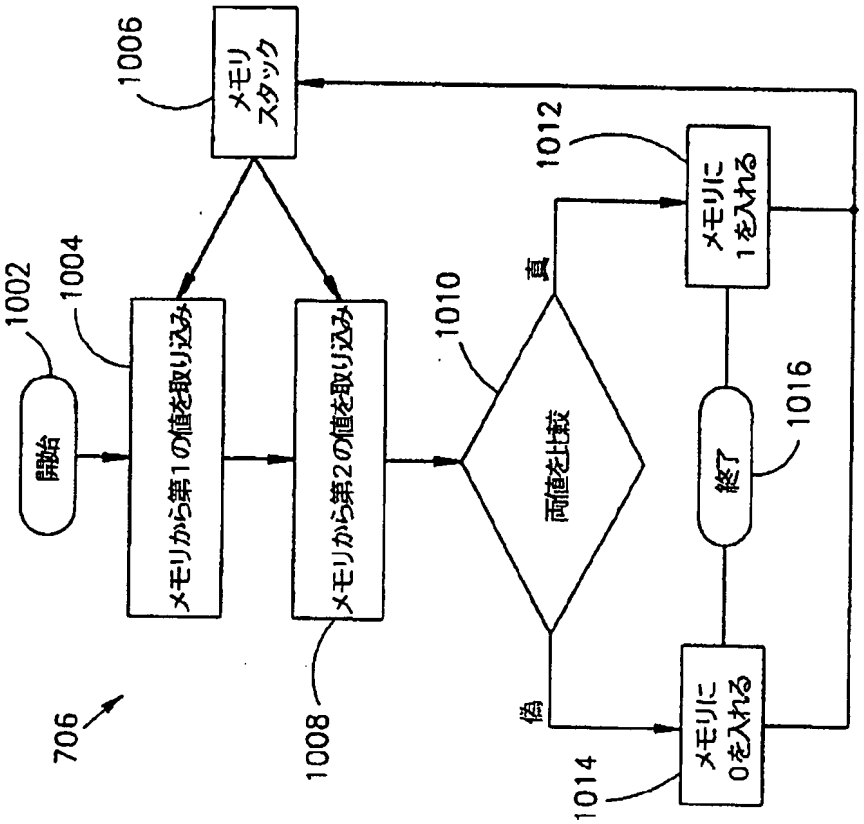


FIG.10

【図１１】

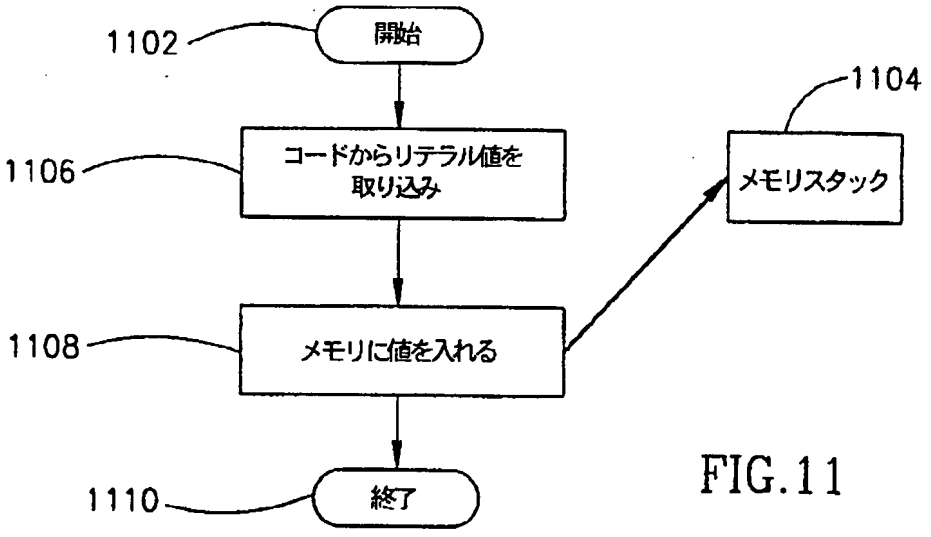


FIG.11

【図１２】

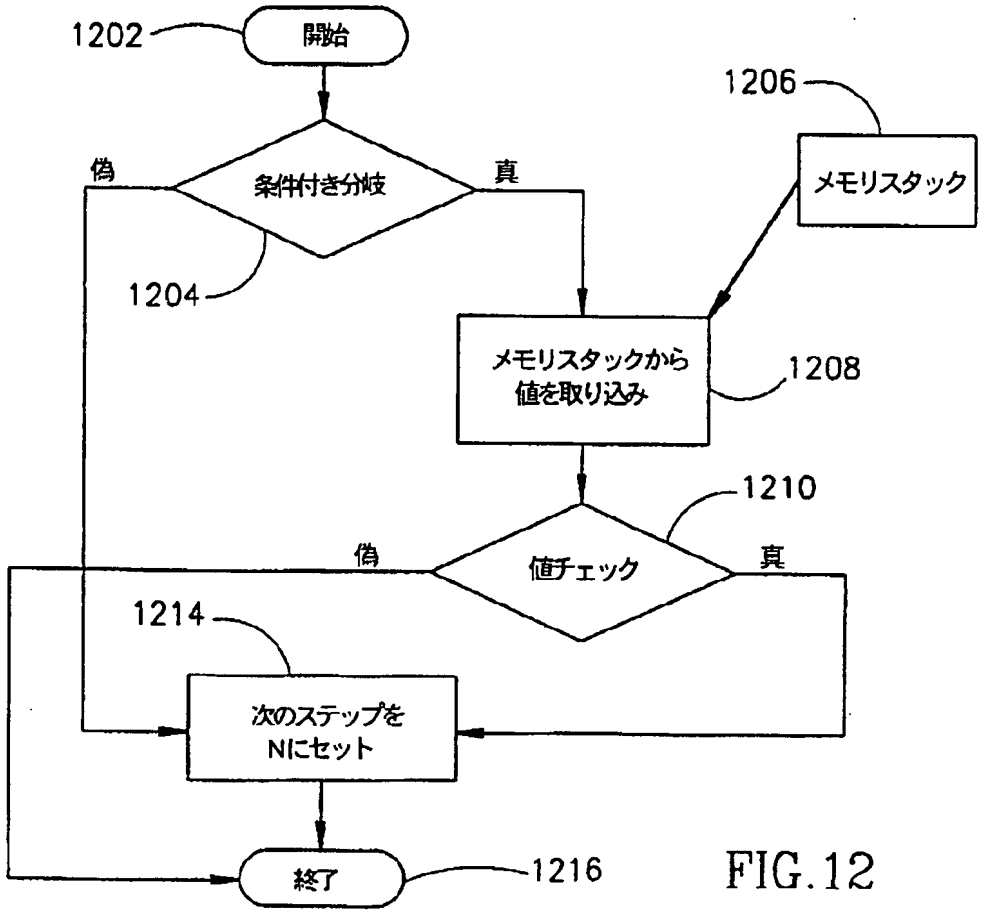

1202
開始
1206
メモリスタック
偽
条件付き分岐
真
1204
メモリスタックから
値を取り込み
1208
1210
偽
値チェック
真
1214
次のステップを
Nにセット
終了
1216

FIG.12

【図１３】

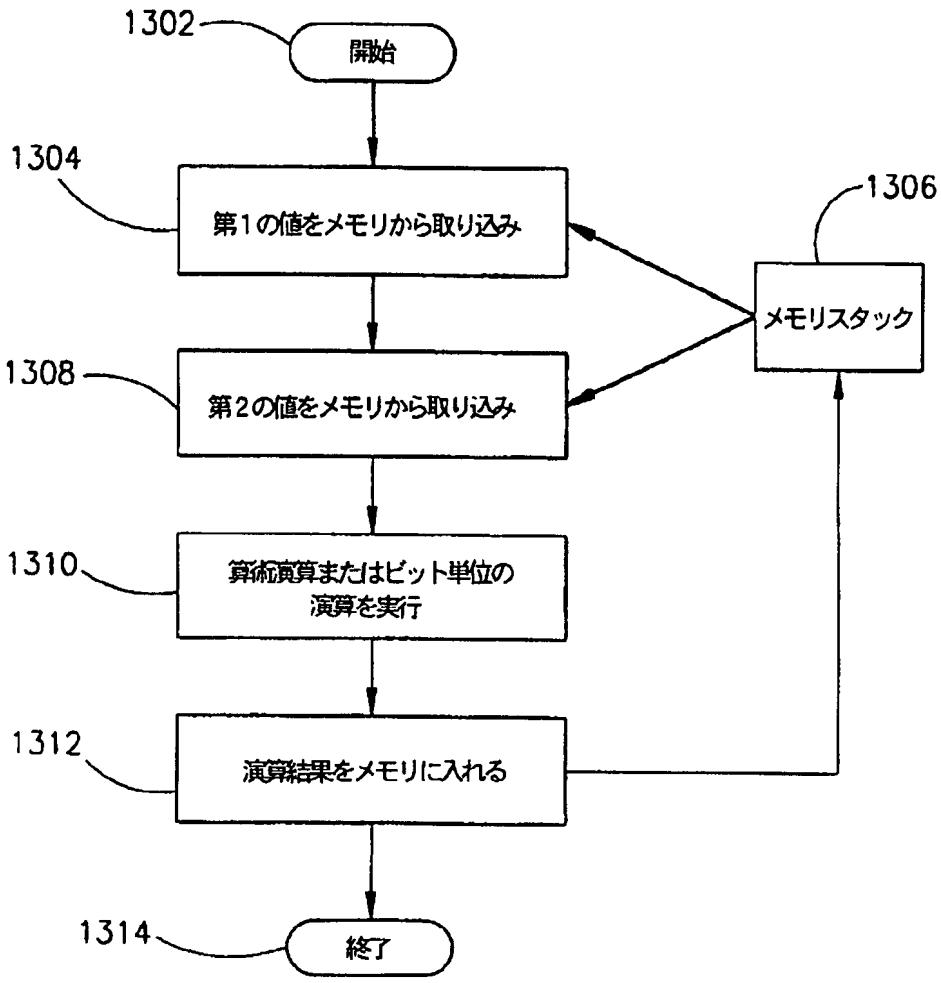

1302
開始
1304
第1の値をメモリから取り込み
1306
メモリスタック
1308
第2の値をメモリから取り込み
1310
算術演算またはビット単位の
演算を実行
1312
演算結果をメモリに入れる
1314
終了

FIG.13

【図１４】

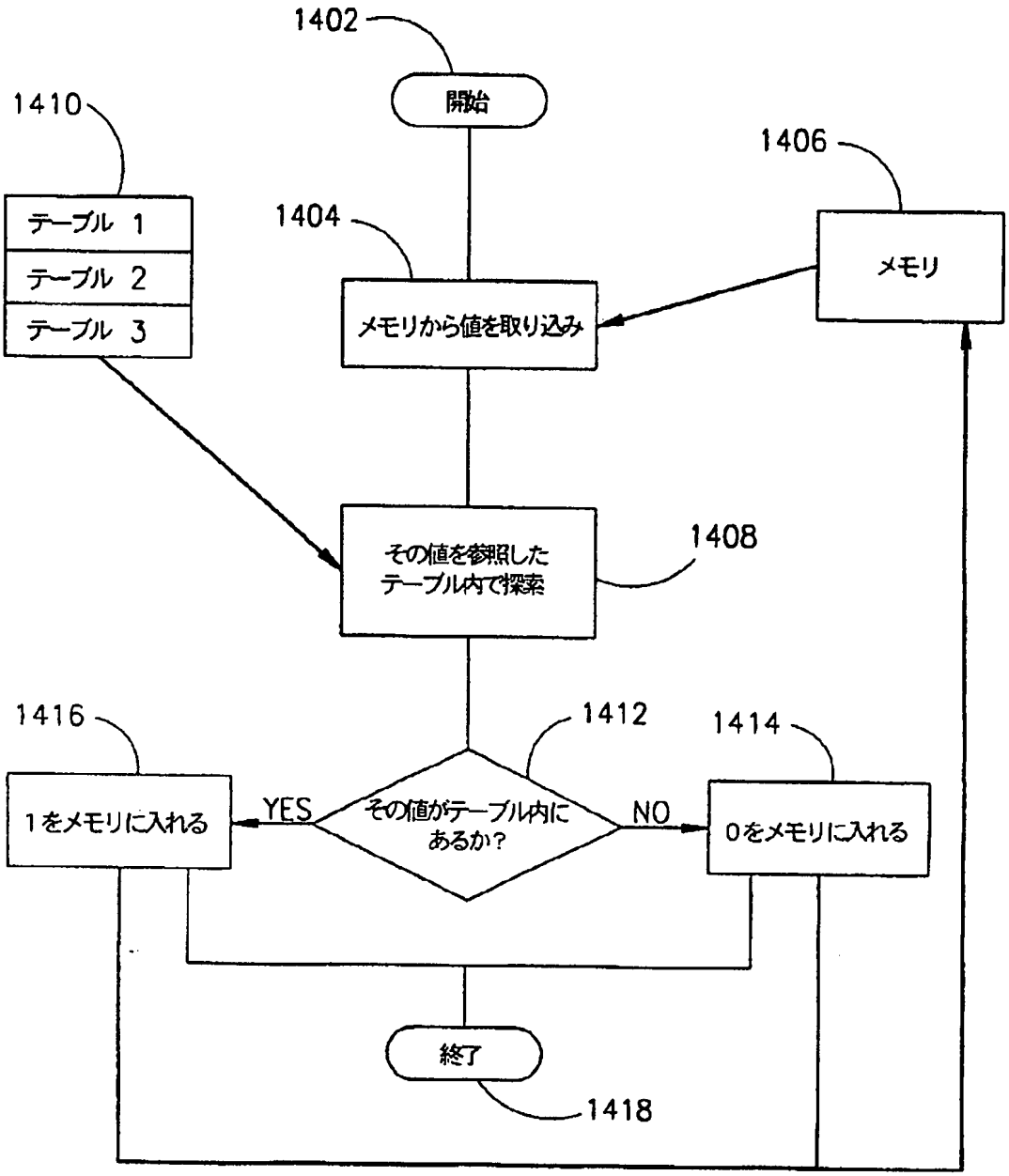

1402
開始
1410
テーブル 1
テーブル 2
テーブル 3
1404
メモリから値を取り込み
1406
メモリ
その値を参照した
テーブル内で探索
1408
1416
1412
1414
1をメモリに入れる
YES
その値がテーブル内に
あるか？
NO
0をメモリに入れる
終了
1418

FIG.14

【図１５】

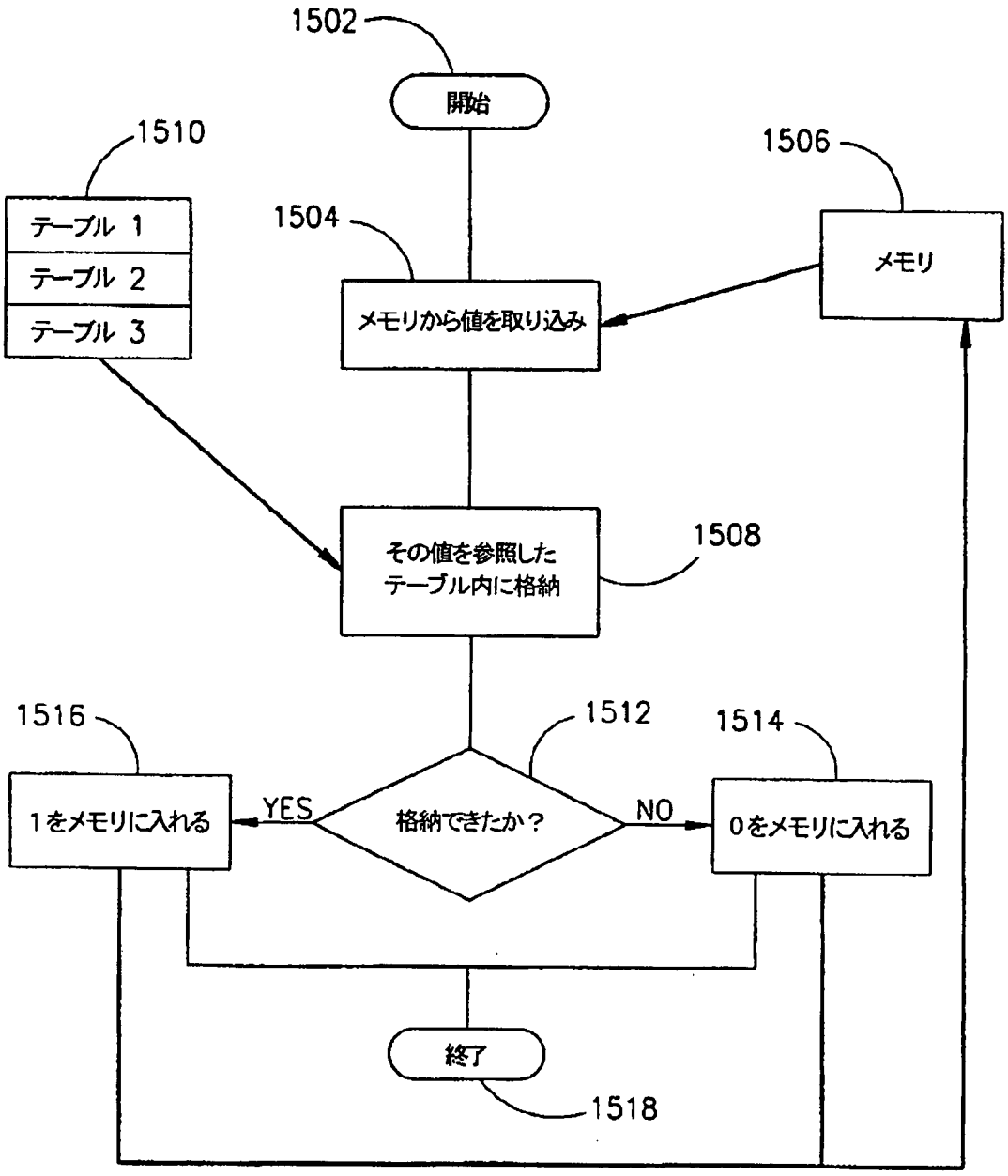

1502
開始
1510
テーブル 1
テーブル 2
テーブル 3
1504
メモリから値を取り込み
1506
メモリ
その値を参照した
テーブル内に格納
1508
1516
1512
1514
1をメモリに入れる
YES
格納できたか？
NO
0をメモリに入れる
終了
1518

FIG.15

【図１６】

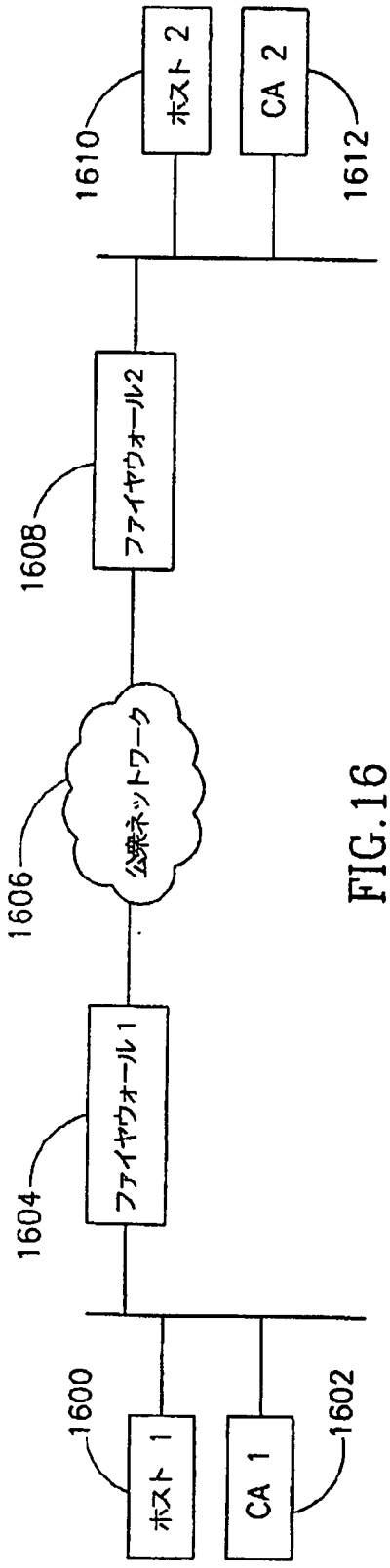

ホスト 2
CA 2
1610
1612
ファイヤウォール2
1608
公衆ネットワーク
1606
ファイヤウォール 1
1604
ホスト 1
CA 1
1600
1602

FIG.16

【図２１】

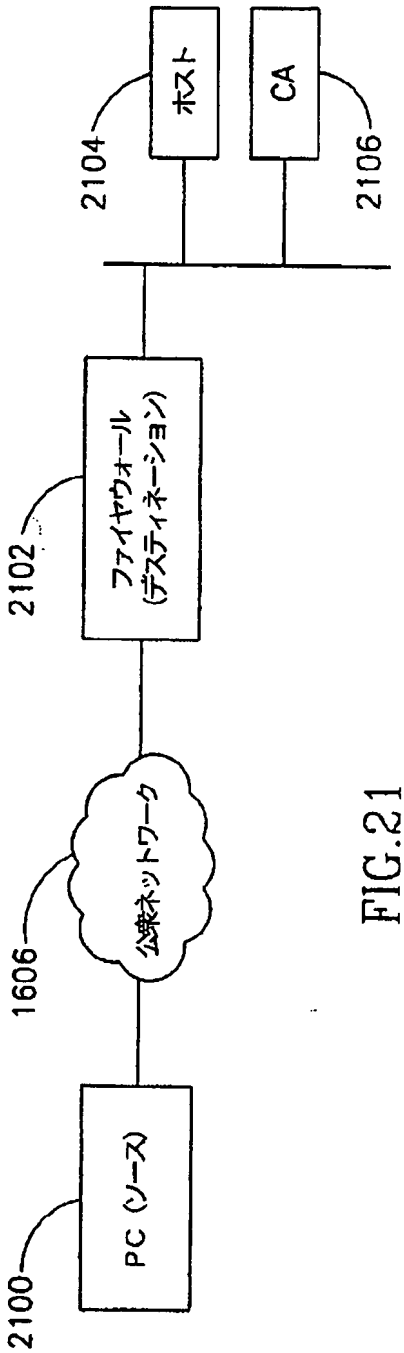

2100
PC (ソース)
1606
公衆ネットワーク
2102
ファイヤウォール
(デスティネーション)
2104
ホスト
2106
CA

FIG.21

【図１７】

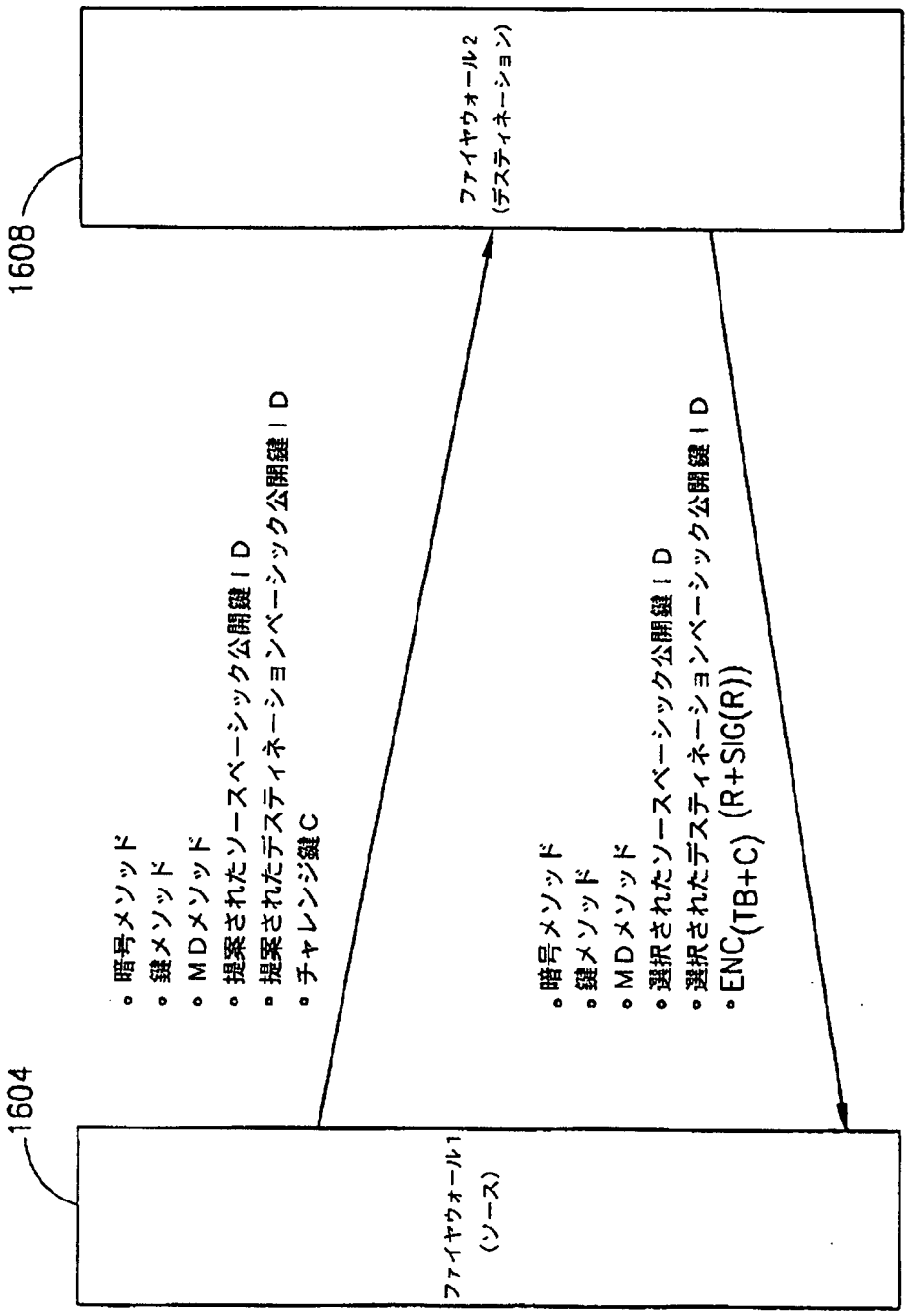

1604
ファイヤウォール1
(ソース)
1608
ファイヤウォール2
(デスティネーション)
・暗号メソッド
・鍵メソッド
・MDメソッド
・提案されたソースベーシック公開鍵ID
・提案されたデスティネーションベーシック公開鍵ID
・チャレンジ鍵C
・暗号メソッド
・鍵メソッド
・MDメソッド
・選択されたソースベーシック公開鍵ID
・選択されたデスティネーションベーシック公開鍵ID
・ENC(TB+C) (R+SIG(R))

FIG.17

【図１８】

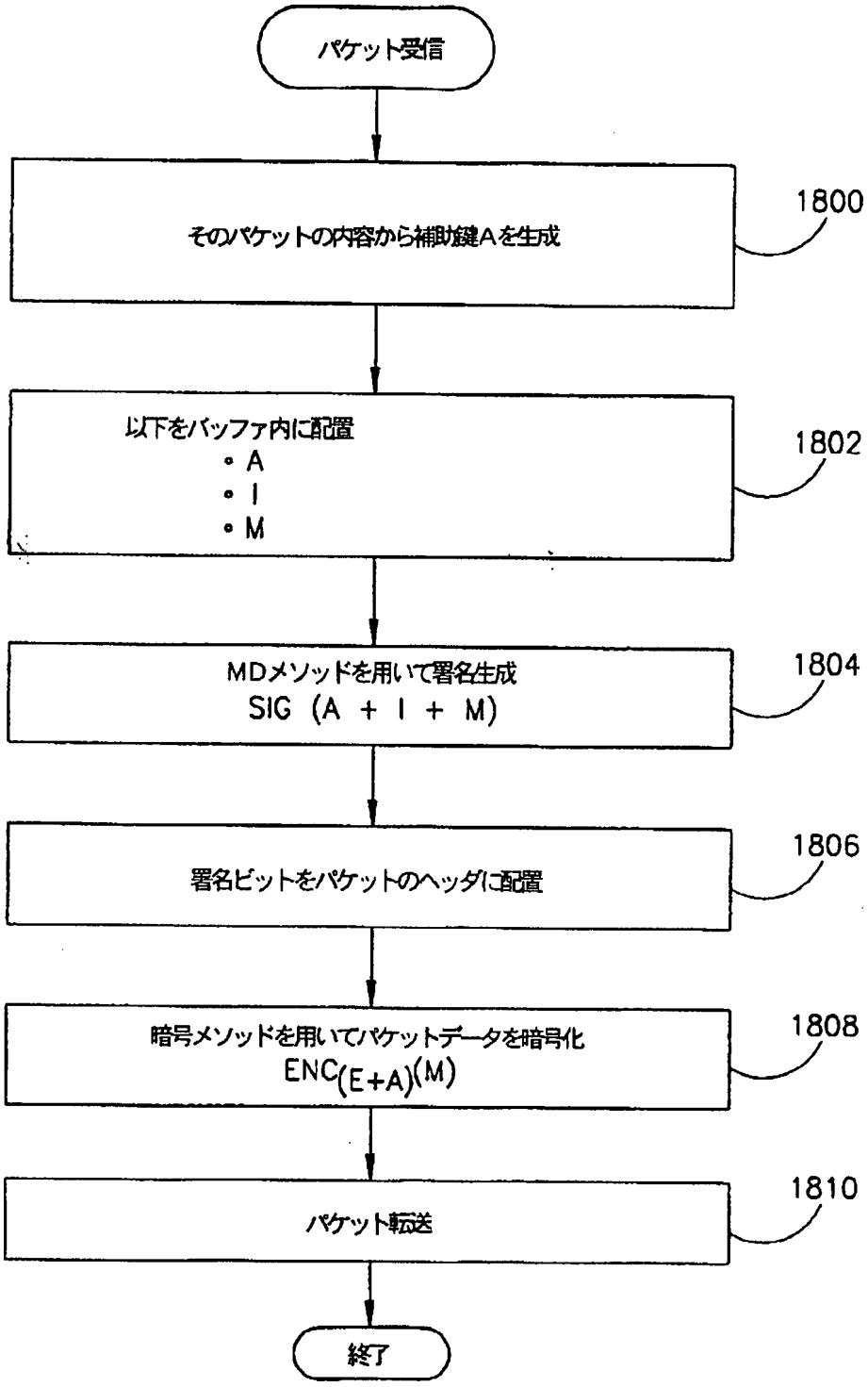

パケット受信
そのパケットの内容から補助鍵Aを生成
1800
以下をバッファ内に配置
• A
• I
• M
1802
MDメソッドを用いて署名生成
SIG (A + I + M)
1804
署名ビットをパケットのヘッダに配置
1806
暗号メソッドを用いてパケットデータを暗号化
ENC(E+A)(M)
1808
パケット転送
1810
終了

FIG.18

【図１９】

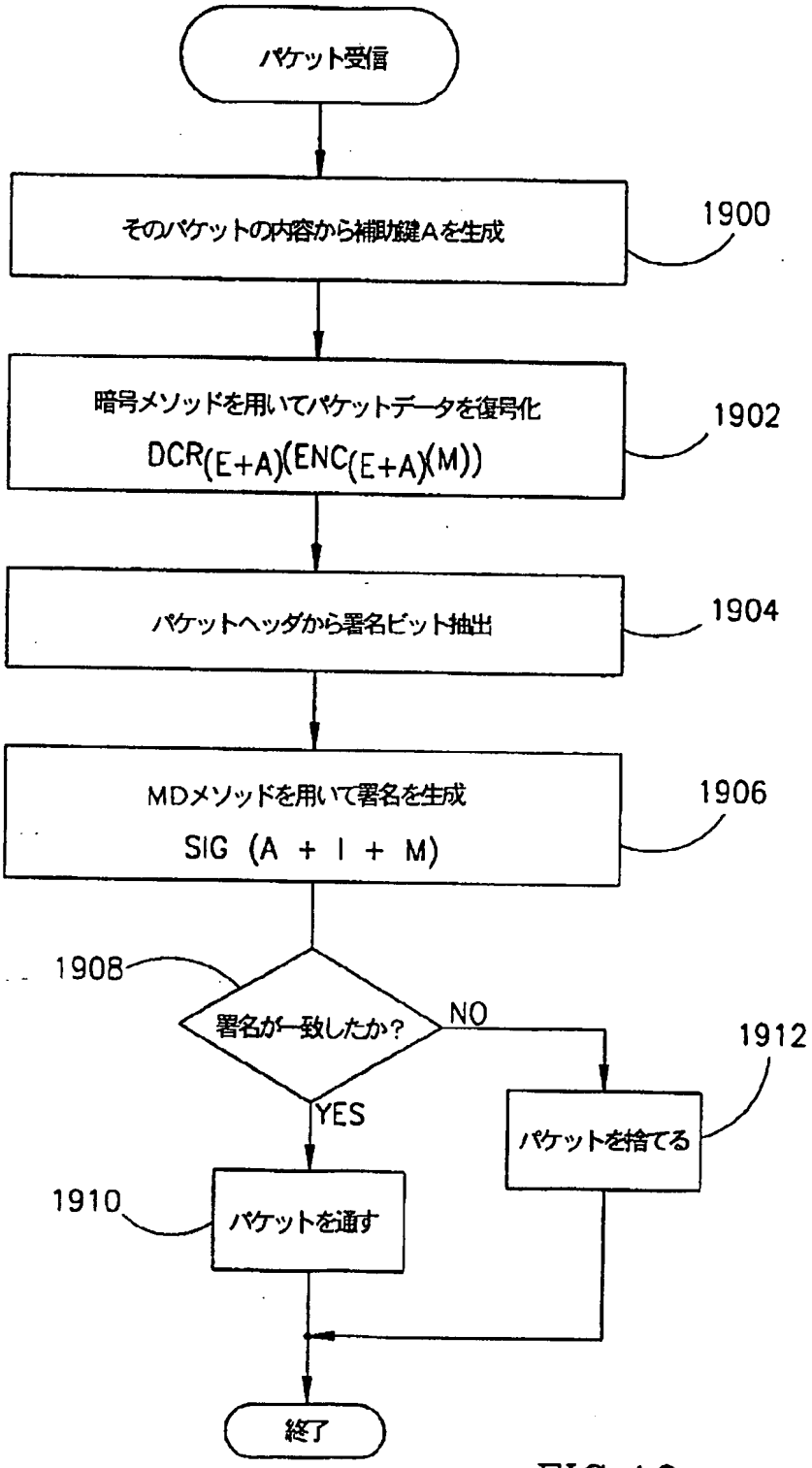

パケット受信
そのパケットの内容から補助鍵Aを生成
1900
暗号メソッドを用いてパケットデータを復号化
DCR(E+A)(ENC(E+A)(M))
1902
パケットヘッダから署名ビット抽出
1904
MDメソッドを用いて署名を生成
SIG (A + I + M)
1906
1908
署名が一致したか?
NO
1912
YES
パケットを捨てる
1910
パケットを通す
終了

FIG.19

【図２０】

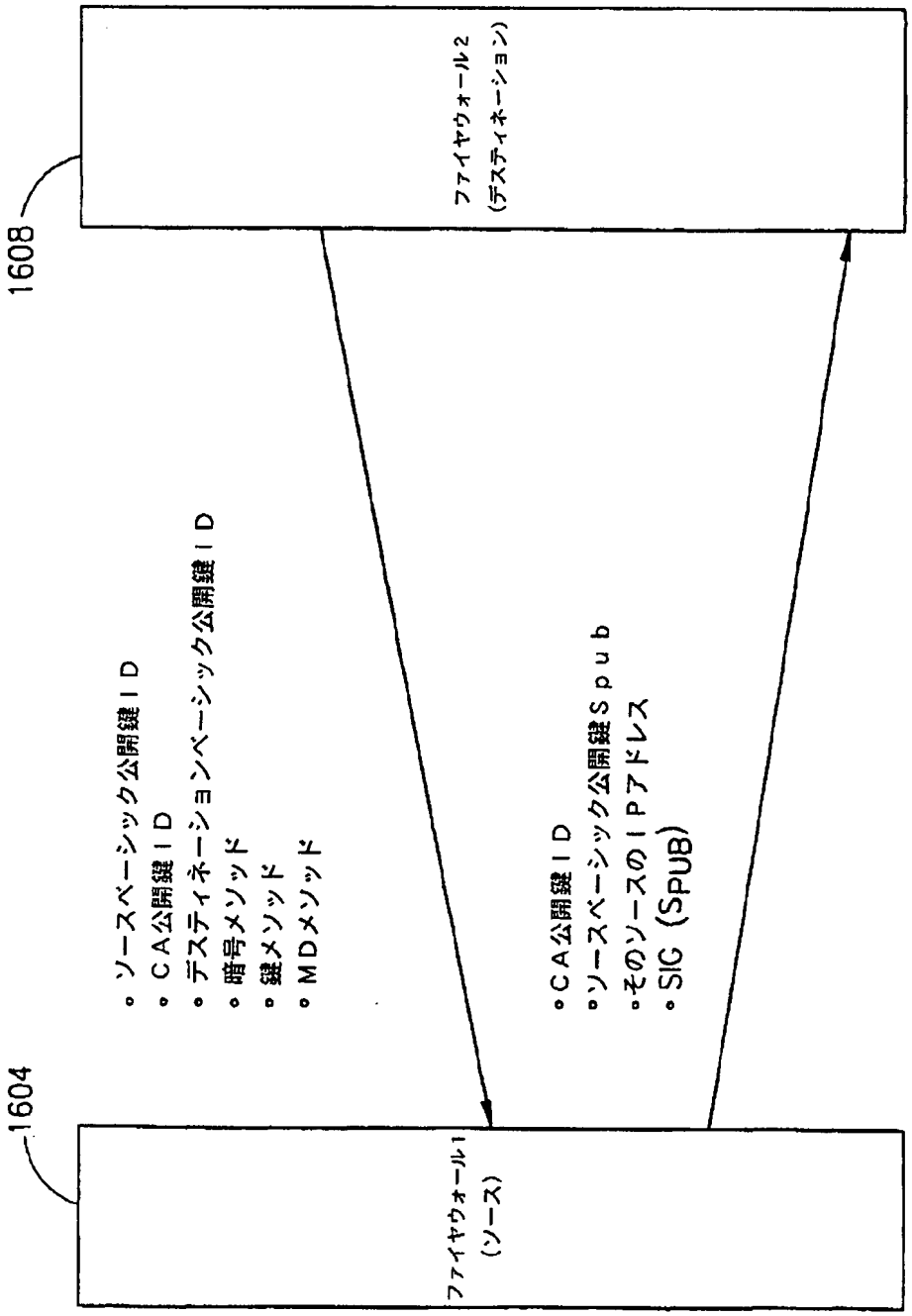

1608
ファイヤウォール2
(デスティネーション)
1604
ファイヤウォール1
(ソース)
・ソースベーシック公開鍵ＩＤ
・ＣＡ公開鍵ＩＤ
・デスティネーションベーシック公開鍵ＩＤ
・暗号メソッド
・鍵メソッド
・ＭＤメソッド
・ＣＡ公開鍵ＩＤ
・ソースベーシック公開鍵Ｓｐｕｂ
・そのソースのＩＰアドレス
・SIG (SPUB)

FIG.20

【図２２】

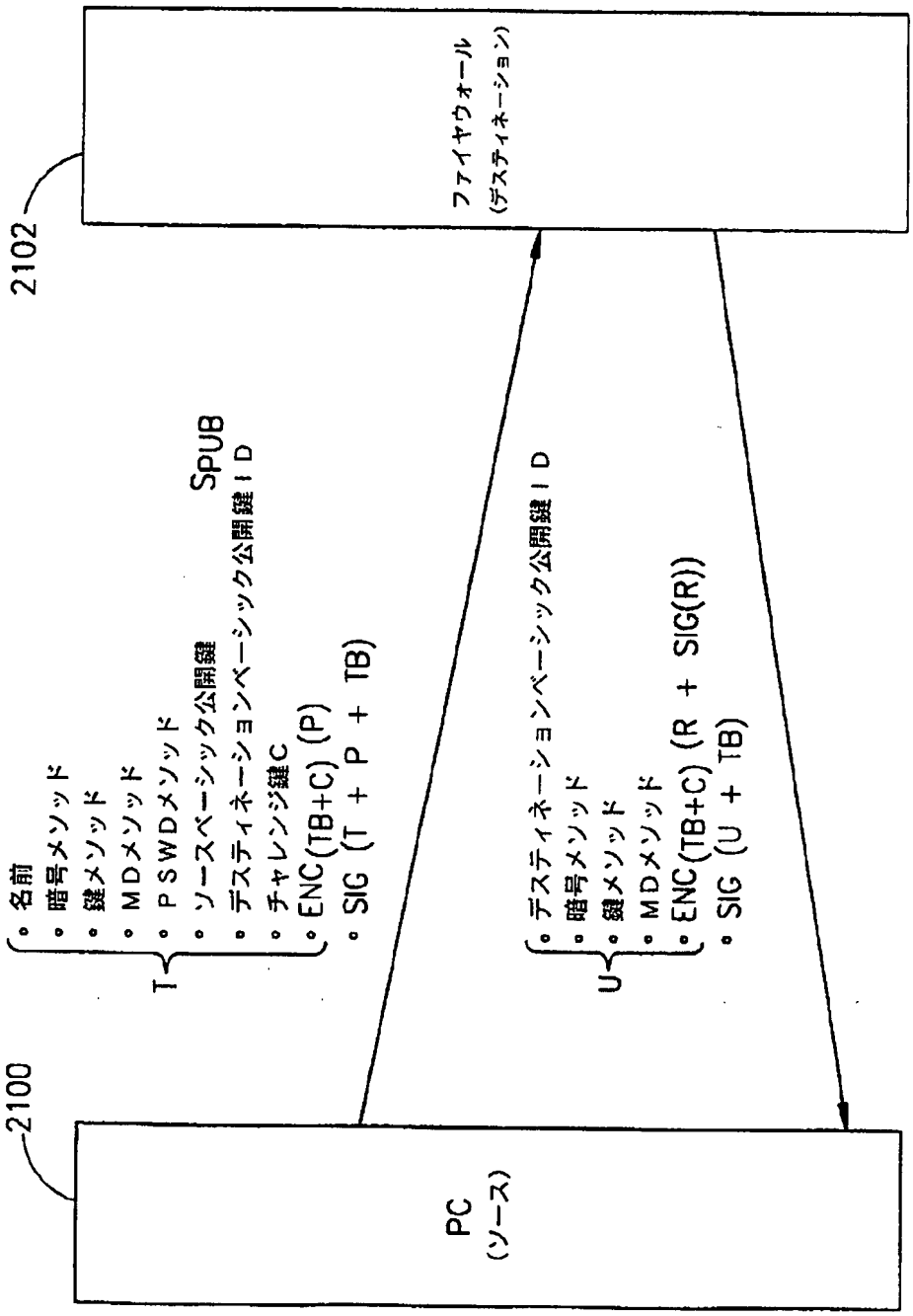

2102
ファイヤウォール
(デスティネーション)
SPUB
T
名前
暗号メソッド
鍵メソッド
MDメソッド
PSWDメソッド
ソースベーシック公開鍵
デスティネーションベーシック公開鍵ID
チャレンジ鍵C
ENC(TB+C) (P)
SIG (T + P + TB)
U
デスティネーションベーシック公開鍵ID
暗号メソッド
鍵メソッド
MDメソッド
ENC(TB+C) (R + SIG(R))
SIG (U + TB)
2100
PC
(ソース)

FIG.22

【図２３】

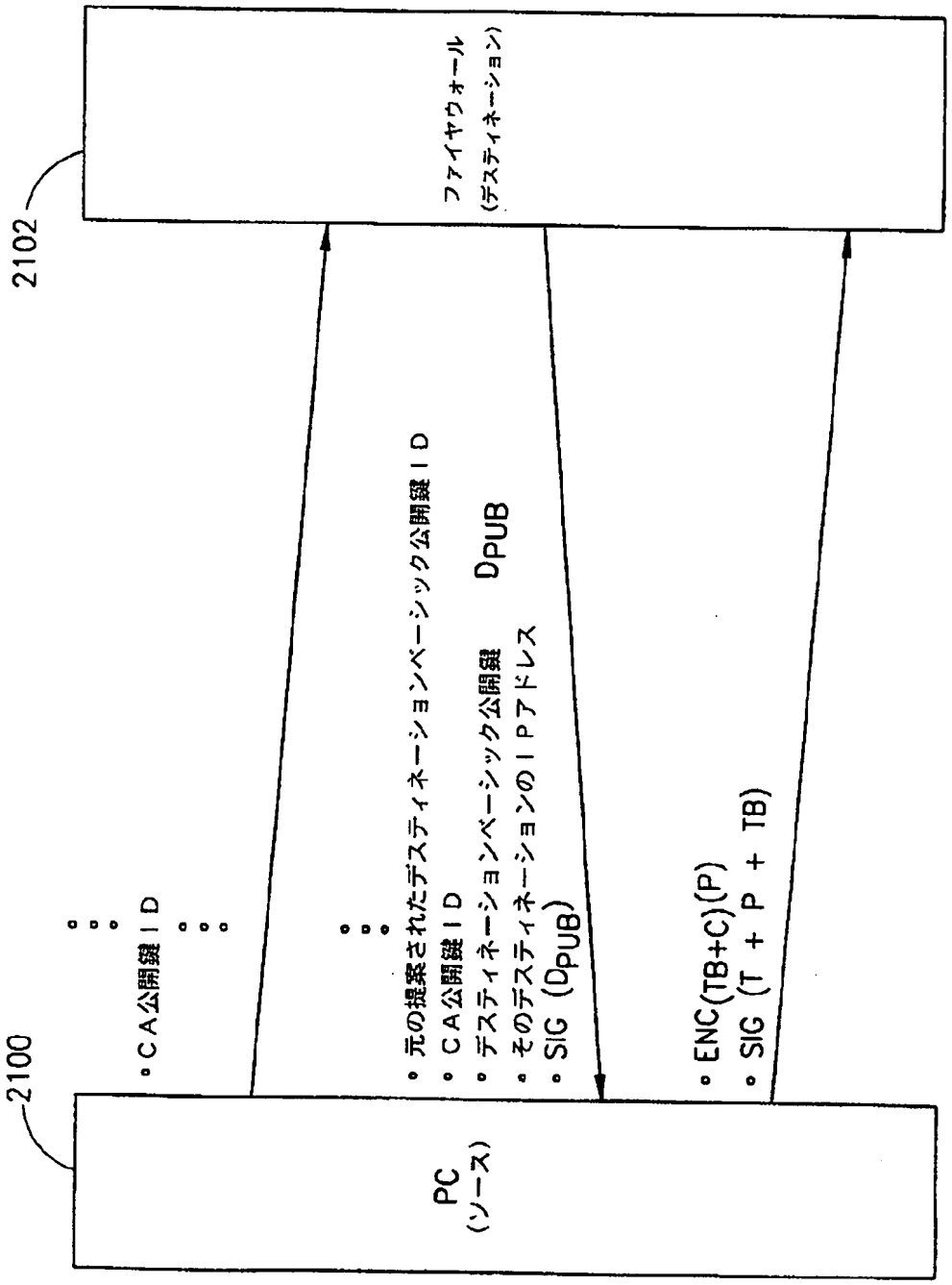

2102
ファイヤウォール
(デスティネーション)
2100
PC
(ソース)
・CA公開鍵ＩＤ
・元の提案されたデスティネーションベーシック公開鍵ＩＤ
・CA公開鍵ＩＤ
・デスティネーションベーシック公開鍵 DPUB
・そのデスティネーションのＩＰアドレス
・SIG (DPUB)
・ENC(TB+C)(P)
・SIG (T + P + TB)

FIG.23

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL96/00017

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00, 12/56
US CL :395/187.01
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 395/187.01, 200.01, 200.06, 200.09, 200.11, 200.17, 200.18; 370/60, 94.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,247,693 (BRISTOL) 21 September 1993, col. 4, line 43-col. 5, line 33.	1-25
Y, E	US 5,555,346 (GROSS et al.) 10 September 1996, col. 2, line 37-col.3, line 21.	1-25
Y, P	US 5,515,376 (MURTHY et al.) 07 May 1996, col. 2, line 31-col. 3, line 23.	2-5, 10-13, 19-22
Y, P	US 5,473,607 (HAUSMAN et al.) 05 December 1995, col. 3, line 36-col. 4, line 20.	14-16
Y	US 5,329,623 (SMITH et al.) 12 July 1994, col. 2, line 51-col. 3, line 25.	8, 17, 23, 25
A, P	US 5,485,455 (DOBBINS et al.) 16 January 1996, col. 2, line 66-col. 6, line 25.	1, 9, 18, 24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be part of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 DECEMBER 1996	31 JAN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer STEPHEN C. ELMORE Telephone No. (703) 305-9713

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL96/00017

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.: 26 (2nd Clm numbered 12)
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

The claim is indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim.

3. ☒ Claims Nos.: 26 (2nd Clm numbered 12)
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)*

フロントページの続き

(81)指定国　EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

(72)発明者　ズク、ニール
イスラエル国ラマットガン52504・ツビストリート　2
(72)発明者　ドゴン、ギル
イスラエル国ヘルツェリア46743・ハキドマストリート　78
(72)発明者　ベンールーベン、エフド
イスラエル国テルアビブ62486・アルバアラトゾットストリート　11

【要約の続き】

ルベースのルールに従ってフィルタリング処理されることになる。前述の検査エンジンは、パケットを受け取るか拒絶するかを各パケット毎に決定する仮想パケットフィルタリングマシンとして機能する。パケットが拒絶される場合、そのパケットは破棄される。パケットが受容される場合、そのパケットは次いで変更処理を施され得る。変更処理には、暗号化、復号化、署名生成、署名確認、またはアドレス変換が含まれ得る。全てのパケット変更処理はルールベースの内容に従って実行される。本発明においては、2つのファイヤウォール間、またはクランアントとファイヤウォール間の通信を暗号化することにより、コンピュータネットワークのセキュリティを更に高めている。これにより、私設ネットワーク及び公衆ネットワークを共にその一部として含むWANにおいて、機密保護されていない公衆ネットワークの使用が可能となり、従って、仮想私設ネットワーク（VPN）を形成できることになる。